

Verordnung zur Durchführung des Fahrpersonalgesetzes (Fahrpersonalverordnung - FPersV)

Art. 1 des Gesetzes vom 27. Juni 2005 (BGBl I, Nr. 40, S. 1882)

Abschnitt 1 Lenk- und Ruhezeiten im nationalen Bereich

§1 Lenk- und Ruhezeiten im Straßenverkehr

(1) Fahrer

1. von Fahrzeugen, die zur Güterbeförderung dienen und deren zulässiges Gesamtgewicht einschließlich Anhänger oder Sattelanhänger mehr als 2,8 Tonnen und nicht mehr als 3,5 Tonnen beträgt, sowie
2. von Fahrzeugen, die zur Personenbeförderung dienen und die nach ihrer Bauart und Ausstattung geeignet und dazu bestimmt sind, mehr als neun Personen einschließlich Fahrer zu befördern und die im Linienverkehr mit einer Linienlänge bis zu 50 Kilometern eingesetzt sind,

haben Lenkzeiten, Lenkzeitunterbrechungen und Ruhezeiten nach Maßgabe der Artikel 1, 6 Abs. 1 Unterabs. 1 Satz 1, Unterabs. 2 und 4 und Abs. 2, Artikel 7 Abs. 1 und 4 Satz 1, Artikel 8 Abs. 1, 2 und 6, Artikel 9 Unterabs. 2 und Artikel 12 Satz 2 der Verordnung (EWG) Nr. 3820/85 des Rates vom 20. Dezember 1985 über die Harmonisierung bestimmter Sozialvorschriften im Straßenverkehr (ABl. EG Nr. L 370 S. 1, 1986 Nr. L 206 S. 36), die durch die Richtlinie 2003/59/EG des Europäischen Parlaments und des Rates vom 15. Juli 2003 (ABl. EU Nr. L 226 S. 4) geändert worden ist, einzuhalten.

(2) Absatz 1 findet keine Anwendung auf

1. Fahrzeuge, die in § 18 genannt sind,
2. Fahrzeuge, die in Artikel 4 Nr. 4 bis 13 der Verordnung (EWG) Nr. 3820/85 genannt sind,
3. nach § 18 Abs. 2 Nr. 1 der Straßenverkehrs-Zulassungs-Ordnung anerkannte selbstfahrende Arbeitsmaschinen.

(3) Abweichend von Absatz 1 Nr. 2 in Verbindung mit Artikel 7 Abs. 1 und 2 der Verordnung (EWG) Nr. 3820/85 haben Fahrer von Kraftomnibussen im Linienverkehr bei einer Linienlänge bis zu 50 Kilometern Lenkzeitunterbrechungen nach Maßgabe der folgenden Vorschriften einzuhalten:

1. Beträgt der durchschnittliche Haltestellenabstand mehr als drei Kilometer, so ist nach einer Lenkzeit von viereinhalb Stunden eine Unterbrechung von mindestens 30 zusammenhängenden Minuten einzulegen. Diese Unterbrechung kann durch zwei Teilunterbrechungen von jeweils mindestens 20 zusammenhängenden Minuten oder drei Teilunterbrechungen von jeweils mindestens 15 Minuten ersetzt werden. Die Teilunterbrechungen müssen innerhalb der Lenkzeit von höchstens viereinhalb Stunden oder teils innerhalb dieser Zeit und teils unmittelbar danach liegen.
2. Beträgt der durchschnittliche Haltestellenabstand nicht mehr als drei Kilometer, sind als Lenkzeitunterbrechungen Arbeitsunterbrechungen ausreichend, soweit diese nach den Dienst- und Fahrplänen in der Arbeitsschicht enthalten sind (z. B. Wendezeiten). Voraussetzung hierfür ist, dass die Gesamtdauer der Arbeitsunterbrechungen mindestens ein Sechstel der vorgesehenen Lenkzeit beträgt. Arbeitsunterbrechungen unter zehn Minuten werden bei der Berechnung der Gesamtdauer nicht berücksichtigt. Durch Tarifvertrag kann vereinbart werden, dass Arbeitsunterbrechungen von mindestens acht Minuten berücksichtigt werden können, wenn ein Ausgleich vorgesehen ist, der die ausreichende Erholung des Fahrers erwarten lässt. Für Fahrer, die nicht in einem Arbeitsverhältnis stehen, kann die nach Landesrecht zuständige Behörde entsprechende Abweichungen bewilligen.

(4) In den Fällen des Absatzes 1 Nr. 2 ist der Fahrer nicht zur Einlegung einer wöchentlichen Ruhezeit nach höchstens sechs Tageslenkzeiten oder bis zum Ende des sechsten Tages verpflichtet, auch wenn die Gesamtlenkzeit während der sechs Tage die Höchstdauer übersteigt, die sechs Tageslenkzeiten entspricht.

FPers 2.2.1

Die Verpflichtung zur Einlegung der wöchentlichen Ruhezeiten bleibt im Übrigen unberührt; jedoch können die wöchentlichen Ruhezeiten auf einen Zweiwochenzeitraum verteilt werden.

(5) Der Unternehmer hat dafür zu sorgen, dass die Vorschriften über die Lenkzeiten, die Lenkzeitunterbrechungen und die Ruhezeiten gemäß den Artikeln 6,7 Abs. 1, 2,4 und 5 sowie den Artikeln 8, 9 und 12 der Verordnung (EWG) Nr. 3820/85 eingehalten werden. Artikel 15 der Verordnung (EWG) Nr. 3820/85 findet entsprechende Anwendung.

(6) Fahrer der in Absatz 1 Nr. 1 genannten Fahrzeuge müssen, sofern diese Fahrzeuge nicht nach Absatz 2 ausgenommen sind, Aufzeichnungen über Lenkzeiten, alle sonstigen Arbeitszeiten, die Lenkzeitunterbrechungen und die Ruhezeiten gemäß den Sätzen 3 bis 5 führen. Der Unternehmer händigt dem Fahrer entsprechende Vordrucke aus. Der Fahrer hat die Aufzeichnungen für jeden Tag getrennt zu fertigen. Die Fahrer müssen jedes Blatt der Aufzeichnungen mit Vor- und Zuname, dem Datum, den amtlichen Kennzeichen der benutzten Fahrzeuge, dem Ort des Fahrtbeginns und des Fahrtendes sowie den Kilometerständen der benutzten Fahrzeuge bei Fahrtbeginn und Fahrtende versehen. Der Fahrer hat alle Eintragungen jeweils unverzüglich zu Beginn und Ende der Lenkzeiten, Lenkzeitunterbrechungen und Ruhezeiten vorzunehmen. Die Fahrer haben die Aufzeichnungen der laufenden Woche und des letzten Tages der Vorwoche, an dem sie ein nachweispflichtiges Fahrzeug gefahren haben, mitzuführen und den zuständigen Personen auf Verlangen zur Prüfung auszuhändigen. Hat der Fahrer in der laufenden Woche oder am letzten Fahrtag der Vorwoche ein Fahrzeug gelenkt, für das die Verordnung (EWG) Nr. 3821/85 des Rates vom 20. Dezember 1985 über das Kontrollgerät im Straßenverkehr (ABl. EG Nr. L 370 S. 8) in der jeweils geltenden Fassung oder das Europäische Übereinkommen vom 1. Juli 1970 über die Arbeit des im internationalen Straßenverkehr beschäftigten Fahrpersonals (AETR) (BGBl. 1974 II S. 1473) in der jeweils geltenden Fassung gilt, ist Satz 6 mit der Maßgabe anzuwenden, dass insoweit die in Artikel 15 der Verordnung (EWG) Nr. 3821/85 oder in Artikel 11 des Anhangs zum AETR vorgeschriebenen Nachweise an Stelle der Aufzeichnungen treten. Anschließend hat der Fahrer die Aufzeichnungen dem Unternehmer unverzüglich auszuhändigen. Der Unternehmer hat die Aufzeichnungen ein Jahr lang aufzubewahren und berechtigten Personen auf Verlangen vorzulegen. Der Unternehmer hat die Aufzeichnungen wöchentlich, im Falle der Verhinderung unverzüglich nach Wegfall des Hinderungsgrundes, zu prüfen und unverzüglich Maßnahmen zu ergreifen, die notwendig sind, um die Beachtung der Sätze 1 bis 7 zu gewährleisten. Die Aufzeichnungspflichten nach den Sätzen 1, 3 und 4 sind erfüllt, wenn die Aufzeichnungen auf einem Vordruck nach Muster der Anlage 1 getätigt werden.

(7) Ist das Fahrzeug mit einem Kontrollgerät nach Anhang I oder I B zur Verordnung (EWG) Nr. 3821/85 oder einem Fahrtschreiber gemäß § 57a der Straßenverkehrs-Zulassungs-Ordnung ausgerüstet, haben Fahrer der in Absatz 1 Nr. 1 genannten Fahrzeuge diese entsprechend den Artikeln 13, 14 Abs. 1 Unterabs. 2, Abs. 4 Buchstabe a Unterabs. 3 Satz 2 oder 3, Artikel 15 Abs. 1 Unterabs. 1 Satz 1 oder 2, Abs. 2 Unterabs. 1 Satz 1, Unterabs. 2 oder 3, Abs. 3, 5a und 7, Artikel 16 Abs. 2 Unterabs. 1 und Abs. 3 der Verordnung (EWG) Nr. 3821/85 oder § 57a Abs. 2 der Straßenverkehrs-Zulassungs-Ordnung zu betreiben. Im Falle der Verwendung eines Fahrtschreibers gemäß § 57a der Straßenverkehrs-Zulassungs-Ordnung hat der Fahrer die Schicht und die Pausen jeweils bei Beginn und Ende für jeden Fahrer auf dem Schaublatt besonders zu vermerken. Der Unternehmer hat bei Verwendung eines Fahrtschreibers dem Fahrer vor Beginn der Fahrt Schaublätter in ausreichender Anzahl auszuhändigen; Absatz 6 Satz 5 bis 10 gilt entsprechend. Hat der Fahrer eines mit einem Kontrollgerät nach Anhang I B zur Verordnung (EWG) Nr. 3821/85 ausgerüsteten Fahrzeugs in der laufenden Woche oder am letzten Fahrtag der Vorwoche ein Fahrzeug gelenkt, das mit einem Kontrollgerät nach Anhang I zur Verordnung (EWG) Nr. 3821/85 ausgerüstet ist, hat er insoweit ebenfalls die Schaublätter während der Fahrt mitzuführen und den Kontrollbeamten auf Verlangen zur Prüfung auszuhändigen.

(8) Weitergehende arbeitsrechtliche Beschränkungen und Pflichten zugunsten der Arbeitnehmer bleiben unberührt.

(9) Unberührt bleibt die Pflicht des Kraftfahrzeugführers, das Fahrzeug nur zu lenken, solange er in der Lage ist, es sicher zu führen.

§ 2

Kontrollgerät nach Anhang I B zur Verordnung (EWG) Nr. 3821/85

(1) Ein Fahrer, der ein Fahrzeug lenkt, das in den Anwendungsbereich der Verordnung (EWG) Nr. 3820/85 fällt, oder der Lenk- oder Ruhezeiten nach § 1 dieser Verordnung einzuhalten hat und dabei ein Kontrollgerät gemäß Anhang I B zur Verordnung (EWG) Nr. 3821/85 betreibt, hat das Kontrollgerät entsprechend den Artikeln 13, 14 Abs. 1 Unterabs. 2, Abs. 4 Buchstabe a Unterabs. 3 Satz 2 oder 3, Artikel 15 Abs. 1 Unterabs. 1 Satz 1 oder 2, Abs. 2 Unterabs. 1 Satz 1, Unterabs. 2 oder 3, Abs. 3, 5a und 7, Artikel 16 Abs. 2 Unterabs. 1 und Abs. 3 der Verordnung (EWG) Nr. 3821/85 zu bedienen und die Benutzerführung zu beachten.

(2) Die in Artikel 15 Abs. 3 zweiter Gedankenstrich Buchstabe b bis d der Verordnung (EWG) Nr. 3821/85 genannten Zeiträume müssen bei Übernahme des Fahrzeugs auf der Fahrerkarte unter Benutzung der im Kontrollgerät vorgesehenen manuellen Eingabemöglichkeiten eingetragen werden, wenn der Fahrer vor Übernahme des Fahrzeugs solche Zeiten verbracht hat.

(3) Wenn die Fahrerkarte beschädigt ist, Fehlfunktionen aufweist oder sich nicht im Besitz des Fahrers befindet, hat der Fahrer zu Beginn seiner Fahrt die Angaben zu dem von ihm verwendeten Fahrzeug auszudrucken, auf diesem Ausdruck Geburts- und Familiennamen und Vornamen sowie die Nummer der Fahrerkarte oder des Führerscheins einzutragen, seine Unterschrift anzubringen sowie die in Artikel 15 Abs. 3 zweiter Gedankenstrich Buchstabe b bis d der Verordnung (EWG) Nr. 3821/85 genannten Zeiten einzutragen. Am Ende seiner Fahrt hat der Fahrer die von dem Kontrollgerät aufgezeichneten Zeiten auszudrucken, auf dem Ausdruck die Zeiten der nicht als Fahrtätigkeit geltenden Tätigkeiten, die seit dem Ausdruck zu Beginn der Fahrt durchgeführt worden sind, Geburts- und Familiennamen und Vornamen sowie die Nummer der Fahrerkarte oder des Führerscheins einzutragen und seine Unterschrift anzubringen. Die Ausdrucke sind den zuständigen Kontrollbeamten vom Fahrer auf Verlangen vorzulegen. Die Ausdrucke sind vom Unternehmer zwei Jahre aufzubewahren und den zuständigen Kontrollbeamten auf Verlangen vorzulegen.

(4) Bei Einsatz von Mietfahrzeugen, deren Verwendung in den Anwendungsbereich der Verordnung (EWG) Nr. 3820/85 oder dieser Verordnung fällt, hat der Unternehmer, der ein Mietfahrzeug anmietet, zu Beginn und am Ende des Mietzeitraums durch Verwendung der Unternehmenskarte sicherzustellen, dass die Daten des Fahrzeugspeichers über die mit den Fahrzeugen durchgeführten Fahrten übertragen und bei ihm gespeichert werden. Ist dies in begründeten Ausnahmefällen nicht möglich, ist zu Beginn und am Ende des Mietzeitraums ein Ausdruck wie bei Beschädigung oder Fehlfunktion der Karte zu fertigen. Der Fahrer hat den Ausdruck unverzüglich nach Erhalt an den Unternehmer weiterzuleiten, der ihn aufzubewahren hat.

(5) Der Unternehmer hat sicherzustellen, dass alle Daten aus dem Massenspeicher des Kontrollgerätes spätestens alle drei Monate, beginnend mit dem ersten Tag der Aufzeichnung, zur Speicherung im Betrieb kopiert werden. Der Unternehmer hat sicherzustellen, dass die Daten der Fahrerkarten spätestens alle 28 Tage, beginnend mit dem ersten Tag der Aufzeichnung, zur Speicherung im Betrieb kopiert werden. Der Fahrer hat hierzu dem Unternehmen die Fahrerkarte und die Ausdrucke nach Absatz 3 zur Verfügung zu stellen. Der Unternehmer hat alle sowohl von den Kontrollgeräten als auch von den Fahrerkarten kopierten Daten zwei Jahre lang zu speichern und auf Verlangen einer zur Kontrolle befugten Stelle entweder unmittelbar oder durch Datenfernübertragung oder auf einem durch die zuständige Behörde zu bestimmenden Datenträger zur Verfügung zu stellen. Der Unternehmer hat von allen kopierten Daten unverzüglich Sicherheitskopien zu erstellen, die auf einem gesonderten Datenträger zu speichern sind.

(6) Unternehmen, die Fahrzeuge vermieten, haben dem Mieter des Fahrzeugs diejenigen Daten aus dem Massenspeicher des Kontrollgerätes, die sich auf die vom Mieter durchgeführten Beförderungen beziehen und auf die dieser nicht unmittelbar zugreifen kann,

1. auf dessen Verlangen sowie
2. nach Beendigung des Mietverhältnisses, spätestens drei Monate nach dessen Beginn oder der letzten Datenübermittlung,

zur Verfügung zu stellen. Dabei sind dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen, die insbesondere die Vertraulichkeit, Unversehrtheit und Zurechenbarkeit der Daten gewährleisten; im Falle der Nutzung allgemein zugänglicher Netze sind dem jeweiligen Stand der Technik entsprechende Verschlüsselungsverfahren anzuwenden.

Version 04/2005

**Abschnitt 2
Organisation**

**§ 3
Zertifizierungsinfrastruktur**

Die Aufgaben der für die Umsetzung des Zertifizierungsverfahrens nach der Verordnung (EWG) Nr. 3821/85 verantwortlichen Stellen ergeben sich aus der Anlage 2. Das Bundesministerium für Verkehr, Bau- und Wohnungswesen nimmt die Aufgaben der Aufsichtsbehörde des Mitgliedstaates (D-Member State Authority - D-MSA) wahr. Deutsche Zertifizierungsstelle (D-Certification Authority - D-CA) ist das Kraftfahrt Bundesamt. Die für die Kontrollgerätkartenausgabe zuständigen Behörden oder Stellen (D-Card Issuing Authorities - D-CIAs) werden von den Ländern bestimmt.

**Abschnitt 3
Kontrollsystem nach EG-Verordnungen**

**§ 4
Allgemeines**

(1) Die zum Betrieb des Kontrollgerätes nach Anhang I B zur Verordnung (EWG) Nr. 3821/85 erforderlichen Kontrollgerätkarten (Fahrer-, Werkstatt-, Unternehmens- und Kontrollkarten) werden nach den Mustern gemäß Anhang I B Abschnitt IV zur Verordnung (EWG) Nr. 3821/85 in Verbindung mit Anlage 3 zu dieser Verordnung gefertigt. Fahrer-, Werkstatt- und Unternehmenskarten werden auf Antrag erteilt. Antragsberechtigt sind:

1. für die Fahrerkarte
 - a) inländische Inhaber einer gültigen Fahrerlaubnis nach Muster 1 der Anlage 8 der Fahrerlaubnis-Verordnung,
 - b) im Übrigen Inhaber einer Fahrerlaubnis eines Mitgliedstaates der Europäischen Union oder eines anderen Vertragsstaats des Abkommens über den Europäischen Wirtschaftsraum, die dazu berechtigt, Fahrzeuge zu führen, für die Lenk- und Ruhezeiten nach der Verordnung (EWG) Nr. 3820/85 beziehungsweise § 1 dieser Verordnung zu beachten sind,
2. für die Werkstattkarte die nach § 57b der Straßenverkehrs-Zulassungs-Ordnung anerkannten oder beauftragten Werkstätten, Hersteller von Kontrollgeräten sowie Fahrzeughersteller,
3. für die Unternehmenskarte Unternehmen, deren Fahrpersonal Beförderungen durchführt, die unter die Verordnung (EWG) Nr. 3820/85 fallen, oder das Lenk- und Ruhezeiten nach § 1 dieser Verordnung einzuhalten hat.

Erfolgt der Antrag auf unpersönlichem Weg, ist eine Kopie der nach den §§ 5, 7 oder § 9 jeweils erforderlichen Unterlagen beizufügen. Im Rahmen des Antragsverfahrens hat für Kontrollgerätkarten nach Nummer 1 eine Überprüfung der Identität des Antragstellers sowie der Übereinstimmung der vorgelegten Kopien mit den Originalen stattzufinden.

(2) Die Kontrollgerätkarten werden von den nach Landesrecht zuständigen Behörden oder Stellen ausgegeben.

(3) Der Antrag auf Erneuerung der Fahrer- und Unternehmenskarte darf frühestens sechs Monate, der auf Erneuerung der Werkstattkarte frühestens einen Monat vor Ablauf der Gültigkeit der Karte gestellt werden. Den Anträgen sind die nach den §§ 5, 7 oder § 9 jeweils erforderlichen Unterlagen beizufügen. Inhaber einer Werkstattkarte haben spätestens nach fünf Jahren eine aktuelle Bescheinigung nach § 7 Abs. 2 Nr. 5 und spätestens nach zwei Jahren einen erneuten Schulungsnachweis nach § 7 Abs. 2 Nr. 7 vorzulegen. Die in Satz 3 genannten Fristen beginnen mit dem Datum des letzten Nachweises. Die in Artikel 14 Abs. 4a Unte-

rabs. 5 und 6, Artikel 12 Abs. 1 Unterabs. 3 der Verordnung (EWG) Nr. 3821/85 genannten Fristen beginnen erst mit der vollständigen Vorlage aller nach den §§ 5, 7 oder § 9 erforderlichen Antragsunterlagen und Angaben.

(4) Wird eine Kontrollgerätkarte wegen Beschädigung, Fehlfunktion, Verlust oder Diebstahl einer vorhandenen Karte beantragt, hat der Antragsteller der ausstellenden Behörde oder Stelle vorzulegen:

1. bei Verlust eine schriftliche Erklärung über den Verlust, 2. bei Diebstahl den Nachweis einer Anzeige,
2. bei Diebstahl den Nachweis einer Anzeige,
3. bei Beschädigung oder Fehlfunktion die zu erneuernde Karte.

Dem Antrag sind die nach den §§ 5, 7 oder § 9 jeweils erforderlichen Unterlagen beizufügen. Der Inhaber der Kontrollgerätkarte hat auf Verlangen der Behörde oder Stelle, welche die Ersatzkarte ausstellt, eine Versicherung an Eides statt abzugeben, dass und aus welchen Gründen er die Kontrollgerätkarte nicht zurückgeben kann. Mit Ausstellung der Ersatzkarte verliert die ersetzte Karte ihre Gültigkeit. Eine wiederaufgefundene Karte ist der Behörde zurückzugeben. Beträgt die Restlaufzeit der zu ersetzenden Karte weniger als sechs Monate, ist die Karte zu erneuern. Absatz 3 Satz 5 gilt mit der Maßgabe, dass die Fristen erst beginnen, wenn alle erforderlichen Antragsunterlagen und Angaben vorliegen und die ausstellende Behörde oder Stelle Kenntnis von der Kartenummer erhält.

(5) Bei Verlust einer Kontrollgerätkarte unterrichtet der Karteninhaber unverzüglich die Behörde oder Stelle, welche die Karte erteilt hat. Die Behörde oder Stelle meldet den Verlust dem Kontrollgerätregister beim Kraftfahrt-Bundesamt.

§ 5 Fahrerkarte

(1) Der Antragsteller hat folgende Unterlagen vorzulegen:

1. a) inländische Antragsteller eine Fahrerlaubnis nach Muster 1 der Anlage 8 der Fahrerlaubnis-Verordnung,
b) im Übrigen eine Fahrerlaubnis eines Mitgliedstaates der Europäischen Union oder eines anderen Vertragsstaats des Abkommens über den Europäischen Wirtschaftsraum, die dazu berechtigt, Fahrzeuge zu führen, für die Lenk- und Ruhezeiten nach der Verordnung (EWG) Nr. 3820/85 beziehungsweise § 1 dieser Verordnung zu beachten sind,
2. einen Nachweis über den Wohnsitz im Inland und Anschrift,
3. Nachweise über Geburts- und Familiennamen, Vornamen, Tag und Ort der Geburt sowie
4. ein Lichtbild vor hellem Hintergrund in der Größe 35 mm x 45 mm, das den Antragsteller ohne Kopfbedeckung im Halbprofil zeigt.

(2) Die zuständige Behörde oder Stelle prüft die Richtigkeit und Vollständigkeit der vom Bewerber mitgeteilten Daten.

(3) Jeder Fahrer erhält nur eine Fahrerkarte. Vor der Ausstellung einer Fahrerkarte erfolgen durch die zuständige Behörde oder Stelle Anfragen bei dem zentralen Fahrerlaubnisregister, dem zentralen Kontrollgerätregister und den Fahrerkartenregistern der anderen Mitgliedstaaten der Europäischen Union und der Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum, ob das vorgelegte Führerscheindokument gültig ist und ob dem Antragsteller bereits anderweitig eine Fahrerkarte ausgestellt wurde. Zu diesem Zweck dürfen die nach § 49 Abs. 1 Nr. 1 bis 3, 5 bis 11 und 15 der Fahrerlaubnis-Verordnung vom 18. August 1998 (BGBl. I S. 2214) in der jeweils geltenden Fassung im Fahrerlaubnisregister gespeicherten Daten im automatisierten Verfahren abgerufen werden.

(4) Die Fahrerkarte darf keinem Dritten zur Nutzung überlassen werden. Der Fahrer hat die Fahrerkarte während der Fahrt mitzuführen und den zuständigen Kontrollbeamten auf Verlangen zur Prüfung auszuhändigen.

FPers 2.2.1

(5) Die Gültigkeitsdauer der Fahrerkarte beträgt bei der Erstaussstellung und Erneuerung fünf Jahre. Sie beginnt mit dem Datum der Personalisierung. Bei der Erneuerung auf Grund von Beschädigung oder Fehlfunktion beginnt sie mit dem Datum der Personalisierung. Bei der Erneuerung auf Grund des Ablaufs der Gültigkeitsdauer beginnt die Gültigkeitsdauer der neuen Fahrerkarte mit dem Tag, der dem Tag des Ablaufs der Gültigkeit der vorherigen Fahrerkarte folgt. Wird eine Fahrerkarte ersetzt, entspricht die Gültigkeitsdauer der Gültigkeitsdauer der ersetzten Karte.

§ 6 Mitführen der abgelaufenen Fahrerkarte Fahrerkarte

Der Fahrer hat auch nach Ablauf der Gültigkeit die Fahrerkarte noch mindestens sieben Tage im Fahrzeug mitzuführen. Bei Umtausch der Fahrerkarte entsprechend Artikel 14 Abs. 4 Buchstabe d der Verordnung (EWG) Nr. 3821/85 hat der Fahrer die Ausdrücke seiner Tätigkeiten für die dem Umtausch vorausgehenden sieben Tage ebenfalls sieben Tage mitzuführen.

§ 7 Werkstattkarte

(1) Die Werkstattkarte wird nur erteilt, wenn der Antragsteller als Unternehmer oder die nach Gesetz oder Satzung zur Vertretung berufene Person sowie die verantwortliche Fachkraft (Installateur) fachlich geeignet sind.

(2) Der Antragsteller hat folgende Angaben zu machen und durch Unterlagen nachzuweisen:

1. Name, Anschrift und Sitz der Werkstatt, des Herstellers von Kontrollgeräten oder des Fahrzeugherstellers,
2. Geburts- und Familiennamen, Vornamen, Tag und Ort der Geburt der nach Gesetz oder Satzung zur Vertretung berufenen Person,
3. Gewerbeanmeldung,
4. Geburts- und Familiennamen, Vornamen, Tag und Ort der Geburt sowie die aktuelle Wohnsitzanschrift der verantwortlichen Fachkraft, für die die Werkstattkarte beantragt wird,
5. eine aktuelle Anerkennung oder Beauftragung der Werkstatt nach § 57b der Straßenverkehrs-Zulassungs-Ordnung,
6. Auszug aus dem Gewerbezentralregister zur Vorlage bei der Behörde,
7. einen Schulungsnachweis der verantwortlichen Fachkraft, für die die Werkstattkarte beantragt wird, entsprechend der Richtlinie für die Durchführung von Schulungen der verantwortlichen Fachkräfte, die Prüfungen der Fahrtschreiber und Kontrollgeräte nach § 57b Abs. 3 der Straßenverkehrs-Zulassungs-Ordnung durchführen,
8. schriftliche, von der verantwortlichen Fachkraft handschriftlich zu bestätigende Erklärung über das mit der verantwortlichen Fachkraft, für die die Werkstattkarte beantragt wird, bestehende Arbeitsverhältnis oder eine Kopie des Arbeitsvertrages.

(3) (entfällt)

(4) Die zuständige Behörde oder Stelle stellt durch Abruf beim zentralen Kontrollgerätkartenregister sicher, dass die verantwortliche Fachkraft nur eine Werkstattkarte pro Arbeitsverhältnis erhält.

(5) Die Werkstattkarte wird dem Unternehmen gegen Empfangsbestätigung ausgehändigt. Sie ist Eigentum des Unternehmens. Die zur Benutzung der Werkstattkarte erforderliche persönliche Identifikationsnummer wird der verantwortlichen Fachkraft an ihre Privatanschrift übersandt.

(6) Die Gültigkeitsdauer der Werkstattkarte beträgt ein Jahr. Sie beginnt mit dem Datum der Personalisierung. § 5 Abs. 5 Satz 3 gilt entsprechend.

§ 8

Wegfall von Erteilungsvoraussetzungen

(1) Ist eine der Erteilungsvoraussetzungen nachträglich entfallen, so ist dies unverzüglich der zuständigen Behörde oder Stelle zu melden; die Werkstattkarte ist innerhalb einer von dieser festzusetzenden Frist an sie zurückzugeben. Die zuständige Behörde oder Stelle hat im Falle des Wegfalls der Erteilungsvoraussetzungen, insbesondere im Falle der missbräuchlichen Verwendung, die Rückgabe der Werkstattkarte zu verlangen. Rückgabepflichtig sind sowohl der Unternehmer, die nach Gesetz oder Satzung zur Vertretung berufene Person als auch die verantwortliche Fachkraft. Scheidet die verantwortliche Fachkraft aus der Werkstatt aus, hat der Unternehmer oder die vertretungsberechtigte Person die Werkstattkarte unverzüglich zurückzugeben. Ist dem Unternehmer oder der vertretungsberechtigten Person eine Rückgabe nicht möglich, ist die ausgebende Behörde oder Stelle unverzüglich zu unterrichten.

(2) Wird die Werkstattkarte wegen missbräuchlicher Verwendung zurückgenommen, unterrichtet die zuständige Behörde oder Stelle das Zentrale Kontrollgerätregister beim Kraftfahrt-Bundesamt.

§ 9

Unternehmenskarte

(1) Der Antragsteller hat folgende Angaben zu machen und durch Unterlagen nachzuweisen:

1. Name, Anschrift und Sitz des Unternehmens,
2. Geburts- und Familiennamen, Vornamen, Tag und Ort der Geburt sowie Anschrift des Unternehmers, bei juristischen Personen der nach Gesetz oder Satzung zur Vertretung berufenen Person sowie einer für den Fahrzeugeinsatz verantwortlichen Person,
3. bei Erstausstellung Gewerbeanmeldung.

(2) Die Unternehmenskarten werden an den Unternehmer oder an die für den Fahrzeugeinsatz verantwortliche Person ausgegeben. Der Unternehmer sorgt für die ordnungsgemäße Verwendung der Karten.

(3) Der Unternehmer hat dafür zu sorgen, dass zu Beginn und am Ende des Fahrzeugeinsatzes für das Unternehmen die Unternehmenskarte in das Kontrollgerät eingegeben wird, um den Einsatz des Fahrzeugs dem Unternehmen zuzuordnen.

(4) Die Gültigkeitsdauer der Unternehmenskarte beträgt fünf Jahre. Sie beginnt mit dem Datum der Personalisierung. § 5 Abs. 5 Satz 3 bis 5 gilt entsprechend.

§ 10

Kontrollkarte

Die Kontrollkarten werden an die für die Kontrolle der Sozialvorschriften im Straßenverkehr zuständigen Behörden und Stellen ausgegeben. Die Kontrollkarte weist die Kontrollbehörde aus und ermöglicht das Lesen, Ausdrucken und Herunterladen der im Massespeicher des Kontrollgerätes oder auf Fahrerkarten gespeicherten Daten. Die Gültigkeitsdauer der Kontrollkarte beträgt fünf Jahre.

**Abschnitt 4
Zentrales Kontrollgerätregister**

**§ 11
Führung und Zweckbestimmung des Registers**

(1) Das Kraftfahrt-Bundesamt führt nach § 2 Nr. 4 des Fahrpersonalgesetzes das Zentrale Kontrollgerätregister zum Nachweis der von den zuständigen Behörden oder Stellen ausgegebenen Kontrollgerätregisterkarten im Sinne des Anhangs I B Abschnitt IV zur Verordnung (EWG) Nr. 3821/85. Darin werden erfasst die Identifizierungsdaten der Fahrer, verantwortlichen Fachkräfte, Unternehmen und Behörden, denen Fahrer-, Werkstatt-, Unternehmens- oder Kontrollkarten ausgestellt worden sind, und die Identifizierungsdaten der ausgestellten, abhanden gekommenen und defekten Fahrer-, Werkstatt-, Unternehmens- und Kontrollkarten.

(2) Das Register wird geführt zur Speicherung von Identifizierungsdaten, die erforderlich sind, um feststellen zu können, welche Karten eine Person, ein Unternehmen oder eine Kontrollbehörde besitzt oder welche Karten abhanden gekommen oder beschädigt sind.

**§ 12
Inhalt des Registers**

Im Zentralen Kontrollgerätregister werden gespeichert über

1. Fahrerkarten folgende Daten:
 - a) Geburts- und Familiennamen, Vornamen, Tag und Ort der Geburt, Doktorgrad und Geschlecht,
 - b) Kontrollgerätregisternummer und die vom Chiphersteller eingebrachte Chipkennung,
 - c) Tag des Beginns und des Ablaufs der Gültigkeit der Fahrerkarte,
 - d) Tag der Produktion der Fahrerkarte,
 - e) Status der Fahrerkarte,
 - f) antragsbearbeitende und mitteilende Behörde oder Stelle einschließlich der für die Antragsbearbeitung verantwortlichen Person,
 - g) Fahrerlaubnisnummer einschließlich Ausgabestaat,
 - h) bei Verlust oder Diebstahl das Datum des Abhandenkommens der Fahrerkarte;
2. Werkstattkarten folgende Daten:
 - a) Name und Anschrift der Werkstatt, des Herstellers von Kontrollgeräten oder des Fahrzeugherstellers, bei der Anschrift zusätzlich die statistische Kennziffer des Firmensitzes sowie der Standortgemeinde und des Gemeindeteils,
 - b) Geburts- und Familiennamen, Vornamen, Tag und Ort der Geburt, Doktorgrad und Geschlecht der nach Gesetz oder Satzung zur Vertretung berufenen Person,
 - c) Geburts- und Familiennamen, Vornamen, Tag und Ort der Geburt, Doktorgrad und Geschlecht der Person, auf die die Karte nach § 7 Abs. 2 Nr. 4 ausgestellt wurde,
 - d) Kontrollgerätenummer und die vom Chiphersteller eingebrachte Chipkennung,
 - e) Tag des Beginns und des Ablaufs der Gültigkeit der Werkstattkarte,
 - f) Tag der Produktion der Werkstattkarte,
 - g) Status der Werkstattkarte,
 - h) antragsbearbeitende und mitteilende Behörde oder Stelle einschließlich der für die Antragsbearbeitung verantwortlichen Person,
 - i) bei Verlust oder Diebstahl das Datum des Abhandenkommens der Werkstattkarte;
3. Unternehmenskarten folgende Daten:
 - a) Name des Unternehmens sowie Anschrift, bei der Anschrift zusätzlich die statistische Kennziffer des Firmensitzes sowie der Standortgemeinde und des Gemeindeteils,

- b) Geburts- und Familiennamen, Vornamen, Tag und Ort der Geburt, Doktorgrad und Geschlecht des Unternehmers beziehungsweise bei juristischen Personen der nach Gesetz oder Satzung zur Vertretung berufenen Person, auf die die Karte nach § 9 Abs. 1 Nr. 2 ausgestellt wurde,
 - c) Kontrollgerätartennummer und die vom Chiphersteller eingebrachte Chipkennung,
 - d) Tag des Beginns und des Ablaufs der Gültigkeit der Unternehmenskarte,
 - e) Tag der Produktion der Unternehmenskarte,
 - f) antragsbearbeitende und mitteilende Behörde oder Stelle einschließlich der für die Antragsbearbeitung verantwortlichen Person,
 - g) Status der Unternehmenskarte,
 - h) bei Verlust oder Diebstahl das Datum des Abhandenkommens der Fahrerkarte;
4. Kontrollkarten folgende Daten:
- a) Name der Behörde sowie Anschrift,
 - b) Kontrollgerätartennummer und die vom Chiphersteller eingebrachte Chipkennung,
 - c) Tag des Beginns und des Ablaufs der Gültigkeit der Kontrollkarte,
 - d) Tag der Produktion der Kontrollkarte,
 - e) Status der Kontrollkarte,
 - f) bei Verlust oder Diebstahl das Datum des Abhandenkommens der Kontrollkarte.

§ 13

Löschung von Eintragungen im Zentralen Kontrollgerätartenregister

Die Daten über Kontrollgerätarten werden ein Jahr nach Ablauf der Gültigkeitsdauer gelöscht.

§ 14

Mitteilung an das Zentrale Kontrollgerätartenregister im automatisierten Dialogverfahren

(1) Die für die Antragsbearbeitung zuständige Behörde oder Stelle teilt dem Zentralen Kontrollgerätartenregister unverzüglich die zu speichernden oder zu einer Änderung einer Eintragung führenden Daten im automatisierten Dialogverfahren mit; sie teilt dem Personalisierer die zur Personalisierung notwendigen Daten mit.

(2) Zuständige ausländische Stellen sind berechtigt, Statusänderungen zu Kontrollgerätarten im automatisierten Dialogverfahren an das Zentrale Kontrollgerätartenregister zu übermitteln.

(3) Der Personalisierer teilt dem Zentralen Kontrollgerätartenregister unverzüglich jeweils nach Produktion und Versand einer Kontrollgerätartenkarte eine entsprechende Information hierüber mit.

§ 15

Übermittlung von Daten an inländische Behörden und Stellen durch Abruf im automatisierten Verfahren

Die im Zentralen Kontrollgerätartenregister gespeicherten Daten dürfen an die hierfür zuständigen Behörden und Stellen durch Abruf im automatisierten Verfahren übermittelt werden, soweit dies erforderlich ist

1. für Verwaltungsmaßnahmen auf Grund der Verordnung (EWG) Nr. 3821/85 oder darauf beruhender Rechtsvorschriften,
2. für Verkehrs- oder Grenzkontrollen,
3. für die Verfolgung von Ordnungswidrigkeiten,
4. für die Verfolgung von Straftaten.

§ 16

Übermittlung von Daten an ausländische Behörden und Stellen durch Abruf im automatisierten Verfahren

Die im Zentralen Kontrollgerätregister über Fahrerkarten und Werkstattkarten gespeicherten Daten dürfen an die hierfür zuständigen Behörden und Stellen in den Mitgliedstaaten der Europäischen Union oder den Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum durch Abruf im automatisierten Verfahren übermittelt, werden, soweit dies erforderlich ist

1. für Verwaltungsmaßnahmen auf Grund der Verordnung (EWG) Nr. 3821/85 oder darauf beruhender Rechtsvorschriften,
2. für Verkehrskontrollen,
3. zur Verfolgung von Zuwiderhandlungen gegen Rechtsvorschriften auf dem Gebiet des Straßenverkehrs oder
4. zur Verfolgung von Straftaten, die im Zusammenhang mit dem Straßenverkehr stehen.

§ 17

Einrichtung und Betrieb der automatisierten Abrufverfahren

Die Einrichtung und der Betrieb der automatisierten Abrufverfahren richten sich nach den Bestimmungen des Bundesdatenschutzgesetzes.

Abschnitt 5 Ausnahmen

§ 18

Ausnahmen gemäß Verordnungen (EWG) Nr. 3820/85 und 3821/85

(1) Gemäß Artikel 13 Abs. 1 der Verordnung (EWG) Nr. 3820/85 und Artikel 3 Abs. 2 der Verordnung (EWG) Nr. 3821/85 werden im Geltungsbereich des Fahrpersonalgesetzes folgende Fahrzeugkategorien von der Anwendung der Verordnungen (EWG) Nr. 3820/85 und 3821/85 ausgenommen:

1. Fahrzeuge, die von Behörden für öffentliche Dienstleistungen verwendet werden, die nicht im Wettbewerb mit dem Kraftverkehrsgewerbe stehen;
2. Fahrzeuge, die von Landwirtschafts-, Gartenbau-, Forstwirtschafts- oder Fischereibetrieben zur Güterbeförderung in einem Umkreis von 50 Kilometern vom Standort des Fahrzeugs verwendet werden;
3. Fahrzeuge, die in einem Umkreis von 50 Kilometern vom Standort des Fahrzeugs zum Transport von Tierkörpern, Tierkörperteilen oder Erzeugnissen im Sinne des Tierkörperbeseitigungsgesetzes eingesetzt werden, soweit für diese Rohmaterialien eine Pflicht zur Beseitigung in einer Tierkörperbeseitigungsanstalt besteht;
4. Fahrzeuge, die in einem Umkreis von 50 Kilometern vom Standort des Fahrzeugs für die Beförderung lebender Tiere von den landwirtschaftlichen Betrieben zu den lokalen Märkten oder Schlachthäusern und umgekehrt oder von den Märkten zu den lokalen Schlachthäusern verwendet werden;
5. Fahrzeuge, die in einem Umkreis von 50 Kilometern vom Standort des Fahrzeugs als Verkaufswagen auf örtlichen Märkten oder für den ambulanten Verkauf oder für ambulante Bank-, Wechsel- oder Spargeschäfte verwendet werden und für diese Zwecke besonders ausgestattet sind;
6. Fahrzeuge, die im Rahmen der Religionsausübung, zum Ausleihen von Büchern, Schallplatten oder Kassetten, für kulturelle Veranstaltungen oder für Wanderausstellungen verwendet werden und für diesen Zweck besonders ausgestattet sind;
7. Fahrzeuge, die in einem Umkreis von 50 Kilometern vom Standort des Fahrzeugs zur Beförderung von Material oder Ausrüstungen verwendet werden, die der Fahrer in Ausübung seines Berufes benötigt; Voraussetzung ist, dass das Führen des Fahrzeugs für den Fahrer nicht die Haupttätigkeit darstellt;

8. Fahrzeuge, die ausschließlich auf Inseln mit einer Fläche von nicht mehr als 2 300 Quadratkilometern verkehren, welche mit den übrigen Teilen des Hoheitsgebietes weder durch eine Brücke noch durch eine Furt noch durch einen Tunnel, die von Kraftfahrzeugen benutzt werden können, verbunden sind;
9. Fahrzeuge, die zur Güterbeförderung dienen und elektrisch betrieben werden, sofern diese Fahrzeuge nach den Rechtsvorschriften des Mitgliedstaates, in dem sie zugelassen sind, den Fahrzeugen mit Benzin- oder Dieselmotor, deren höchstzulässiges Gesamtgewicht einschließlich der Anhänger oder der Sattelanhänger 3,5 Tonnen nicht übersteigt, gleichgestellt sind;
10. Fahrzeuge, die zur Ausbildung von Fahrschülern und Fahrlehrern (§ 5 Abs. 1 und § 12 der Durchführungsverordnung zum Fahrlehrergesetz vom 18. August 1998, BGBl. I S. 2307, in ihrer jeweils geltenden Fassung) sowie für die entsprechenden Prüfungen (Anlage 7 zu § 17 Abs. 2 der Fahrerlaubnis-Verordnung vom 18. August 1998, BGBl. I S. 2214, in der jeweils geltenden Fassung und §§ 15 und 18 der Prüfungsordnung für Fahrlehrer vom 18. August 1998, BGBl. I S. 2307, 2331, in der jeweils geltenden Fassung) verwendet werden;
11. Traktoren (Zugmaschinen), die ausschließlich land oder forstwirtschaftlichen Arbeiten dienen;
12. Fahrzeuge, die ausschließlich zur privaten, nicht gewerblichen Personenbeförderung dienen und die nach ihrer Bauart und Ausstattung geeignet und dazu bestimmt sind, bis zu 17 Personen -einschließlich des Fahrers - zu befördern.

(2) Gemäß Artikel 5 Abs. 5 der Verordnung (EWG) Nr. 3820/85 wird für Beförderungen in einem Umkreis von 50 Kilometern vom Standort des Fahrzeugs das Mindestalter der Beifahrer zum Zwecke der Berufsausbildung auf das vollendete 16. Lebensjahr herabgesetzt.

(3) Artikel 6 Abs. 1 Unterabs. 4 der Verordnung (EWG) Nr. 3820/85 findet auch auf den innerstaatlichen Personenverkehr (außer Linienverkehr) auf dem Hoheitsgebiet der Bundesrepublik Deutschland Anwendung.

Abschnitt 6

Europäisches Übereinkommen über die Arbeit des im internationalen Straßenverkehr beschäftigten Fahrpersonals (AETR)

§ 19

Kontrollgeräte nach dem Europäischen Übereinkommen über die Arbeit des im internationalen Straßenverkehr beschäftigten Fahrpersonals (AETR)

Auf Grund des Artikels 3 Abs. 1 und des Artikels 10 Abs. 1 des AETR in Verbindung mit Artikel 2 Abs. 2 der Verordnung (EWG) Nr. 3820/85 hat der Unternehmer in Fahrzeuge, die dem AETR unterliegen und mit denen das Hoheitsgebiet der Bundesrepublik Deutschland befahren wird, vor Antritt derartiger Fahrten Kontrollgeräte einbauen zu lassen. Die Kontrollgeräte nach Satz 1 sind von dem Fahrer zu benutzen. Die Kontrollgeräte sind nach den Artikeln 10 und 11 des Anhangs zum AETR zu betreiben, Bauart, Einbau, Benutzung und Prüfung der Kontrollgeräte richten sich nach den Vorschriften des AETR einschließlich seines Anhangs und der Anlagen, Kontrollgeräte im Sinne der Verordnung (EWG) Nr. 3821/85 erfüllen die Anforderungen nach Satz 4.

Abschnitt 7

Sonstige Vorschriften

§ 20

Nachweis über berücksichtigungsfreie Tage

(1) Fahrer, die die in Artikel 15 Abs. 7 der Verordnung (EWG) Nr. 3821/85 oder Kapitel III Artikel 11 des Anhangs zum AETR sowie dieser Verordnung vorgeschriebenen Schaublätter oder Aufzeichnungen nicht vor-

FPers 2.2.1

legen können, weil sie an diesen Tagen kein Fahrzeug oder nur solche Fahrzeuge gelenkt haben, für deren Führen eine Nachweispflicht nicht besteht, haben dem zuständigen Kontrollbeamten auf Verlangen für die Tage der laufenden Woche eine Bescheinigung des Unternehmers oder einen anderen geeigneten Nachweis vorzulegen. Der Unternehmer hat den betroffenen Fahrern eine solche Bescheinigung vor Fahrtantritt unter Angabe von Gründen auszustellen und auszuhändigen. Die Bescheinigung ist vom Unternehmer oder einer von ihm beauftragten Person zu unterzeichnen.

(2) In den Fällen, in denen eine solche Bescheinigung nicht ausgestellt werden konnte, weil die berücksichtigungsfreien Tage unterwegs angefallen sind, hat der Unternehmer auf Verlangen der Kontrollbehörde nachträglich eine Bescheinigung auszustellen oder vorzulegen.

(3) Artikel 14 Abs. 2 der Verordnung (EWG) Nr. 3821/85 gilt entsprechend.

Abschnitt 8 Ordnungswidrigkeiten

§ 21 Ordnungswidrigkeiten

(1) Ordnungswidrig im Sinne des § 8 Abs. 1 Nr. 1 Buchstabe a des Fahrpersonalgesetzes handelt, wer als Unternehmer vorsätzlich oder fahrlässig

1. entgegen § 1 Abs. 5 Satz 1 nicht dafür sorgt, dass die dort genannten Vorschriften eingehalten werden,
2. entgegen § 1 Abs. 6 Satz 9, auch in Verbindung mit Abs. 7 Satz 3, oder Abs. 6 Satz 10 eine Aufzeichnung oder ein Schaublatt nicht oder nicht mindestens ein Jahr aufbewahrt oder nicht oder nicht rechtzeitig vorlegt, eine Aufzeichnung nicht oder nicht rechtzeitig prüft oder eine Maßnahme nicht oder nicht rechtzeitig ergreift,
3. entgegen § 1 Abs. 7 Satz 3 ein Schaublatt nicht oder nicht rechtzeitig aushändigt,
4. entgegen § 2 Abs. 3 Satz 4 einen Ausdruck nicht oder nicht mindestens 2 Jahre aufbewahrt oder nicht oder nicht rechtzeitig vorlegt,
5. entgegen § 2 Abs. 4 Satz 1 nicht sicherstellt, dass die Daten des Fahrzeugspeichers übertragen und gespeichert werden,
6. entgegen § 2 Abs. 5 Satz 1 oder 2 nicht sicherstellt, dass die dort genannten Daten kopiert werden,
7. entgegen § 2 Abs. 5 Satz 4 Daten nicht oder nicht mindestens zwei Jahre speichert oder nicht oder nicht rechtzeitig zur Verfügung stellt,
8. entgegen § 2 Abs. 5 Satz 5 eine Sicherheitskopie nicht oder nicht rechtzeitig erstellt,
9. entgegen § 2 Abs. 6 Satz 1 Daten nicht oder nicht rechtzeitig zur Verfügung stellt,
10. entgegen § 19 Satz 1 ein Kontrollgerät nicht oder nicht rechtzeitig einbauen lässt oder
11. entgegen § 20 Abs. 1 Satz 2 oder Abs. 2 eine dort genannte Bescheinigung nicht, nicht richtig oder nicht rechtzeitig ausstellt, nicht oder nicht rechtzeitig aushändigt oder nicht oder nicht rechtzeitig vorlegt.

(2) Ordnungswidrig im Sinne des § 8 Abs. 1 Nr. 2 Buchstabe a des Fahrpersonalgesetzes handelt, wer als Fahrer vorsätzlich oder fahrlässig

1. entgegen § 1 Abs. 1 oder 3 Nr. 1 Satz 1 oder Nr. 2 Satz 2 Lenkzeiten, Lenkzeitunterbrechungen oder Ruhezeiten nicht einhält,
2. entgegen § 1 Abs. 6 Satz 1 oder 6, jeweils auch in Verbindung mit Abs. 7 Satz 3, eine Aufzeichnung nicht, nicht richtig oder nicht vollständig führt oder eine Aufzeichnung oder ein Schaublatt nicht mitführt oder nicht oder nicht rechtzeitig aushändigt,
3. entgegen § 1 Abs. 7 Satz 1 ein Kontrollgerät oder einen Fahrtschreiber nicht oder nicht richtig betreibt,

4. entgegen § 1 Abs. 7 Satz 2 die Schicht oder die Pausen auf dem Schaublatt nicht, nicht richtig oder nicht rechtzeitig vermerkt,
5. entgegen § 1 Abs. 7 Satz 4 die Schaublätter nicht mitführt oder nicht oder nicht rechtzeitig zur Prüfung aushändigt,
6. entgegen § 2 Abs. 1 ein Kontrollgerät nicht oder nicht richtig bedient oder die Benutzerführung nicht oder nicht richtig beachtet,
7. entgegen § 2 Abs. 2 einen dort genannten Zeitraum auf der Fahrerkarte nicht, nicht richtig oder nicht rechtzeitig einträgt,
8. entgegen § 2 Abs. 3 Satz 1 oder 2 eine dort genannte Angabe oder eine dort genannte Zeit nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig einträgt oder die Unterschrift nicht oder nicht rechtzeitig anbringt,
9. entgegen § 2 Abs. 3 Satz 3 einen Ausdruck nicht oder nicht rechtzeitig vorlegt,
10. entgegen § 2 Abs. 4 Satz 3 den Ausdruck nicht oder nicht rechtzeitig weiterleitet,
11. entgegen § 5 Abs. 4 Satz 1 die Fahrerkarte einem Dritten zur Nutzung überlässt,
12. entgegen § 5 Abs. 4 Satz 2 die Fahrerkarte nicht mitführt oder nicht oder nicht rechtzeitig zur Prüfung aushändigt,
13. entgegen § 6 die abgelaufene Fahrerkarte oder den Ausdruck nicht oder nicht mindestens sieben Tage mitführt,
14. entgegen § 19 Satz 2 ein Kontrollgerät nicht benutzt oder
15. entgegen § 20 Abs. 1 Satz 1 eine Bescheinigung oder einen Nachweis nicht, nicht richtig oder nicht rechtzeitig vorlegt.

(3) Ordnungswidrig im Sinne des § 8 Abs. 1 Nr. 4 Buchstabe a des Fahrpersonalgesetzes handelt, wer als Werkstattinhaber oder als verantwortliche Fachkraft (Installateur) vorsätzlich oder fahrlässig

1. entgegen § 8 Abs. 1 Satz 1 erster Halbsatz den Wegfall der Erteilungsvoraussetzungen nicht meldet oder
2. entgegen § 4 Abs. 4 Satz 5 oder § 8 Abs. 1 Satz 1 zweiter Halbsatz in Verbindung mit Satz 3 oder 5 eine Werkstattkarte nicht oder nicht rechtzeitig zurückgibt.

§ 22

Zu widerhandlungen gegen die Verordnung (EWG) Nr. 3820/85

(1) Ordnungswidrig im Sinne des § 8 Abs. 1 Nr. 1 Buchstabe b des Fahrpersonalgesetzes handelt, wer als Unternehmer gegen die Verordnung (EWG) Nr. 3820/85 des Rates vom 20. Dezember 1985 über die Harmonisierung bestimmter Sozialvorschriften im Straßenverkehr (ABI. EG Nr. L 370 S. 1, 1986 Nr. L 206 S. 36), die durch die Richtlinie 2003/59/EG des Europäischen Parlaments und des Rates vom 15. Juli 2003 (ABI. EU Nr. L 226 S. 4) geändert worden ist, verstößt, indem er vorsätzlich oder fahrlässig

1. entgegen Artikel 5 Abs. 1, 2 oder 3 einen Fahrer oder Beifahrer einsetzt, der die dort genannten Voraussetzungen nicht erfüllt,
2. entgegen Artikel 6 Abs. 1 Unterabs. 1 Satz 1, Unterabs. 2 oder 4 oder Abs. 2, Artikel 7 Abs. 1 oder 4 Satz 1 oder Artikel 8 Abs. 1, 2 oder 6, jeweils in Verbindung mit Artikel 15 Abs. 1, nicht dafür sorgt, dass die Lenkzeiten, die Lenkzeitunterbrechungen oder die Ruhezeiten eingehalten werden,
3. entgegen Artikel 14 Abs. 1 in Verbindung mit Abs. 2, 3 oder 4 einen Linienfahrplan oder einen Arbeitszeitplan nicht, nicht richtig oder nicht vollständig ausarbeitet oder
4. entgegen Artikel 14 Abs. 6 Satz 1 den Arbeitszeitplan nicht oder nicht mindestens ein Jahr aufbewahrt.

(2) Ordnungswidrig im Sinne des § 8 Abs. 1 Nr. 2 Buchstabe b des Fahrpersonalgesetzes handelt, wer als Fahrer gegen die Verordnung (EWG) Nr. 3820/85 verstößt, indem er vorsätzlich oder fahrlässig

1. entgegen Artikel 5 Abs. 1 oder 2 Unterabs. 1 ein Fahrzeug führt, ohne das dort festgesetzte Mindestalter erreicht zu haben,

FPers 2.2.1

2. entgegen Artikel 5 Abs. 2 Unterabs. 2 ein Fahrzeug führt, ohne den dort festgesetzten Anforderungen zu entsprechen,
3. entgegen Artikel 6 Abs. 1 Unterabs. 1 Satz 1, Unterabs. 2 oder 4 oder Abs. 2, Artikel 7 Abs. 1 oder 4 Satz 1, Artikel 8 Abs. 1, 2 oder 6 oder Artikel 9 Unterabs. 2 die Lenkzeiten, die Lenkzeitunterbrechungen oder die Ruhezeiten nicht einhält,
4. entgegen Artikel 12 Satz 2 Art oder Grund einer Abweichung von den Bestimmungen nicht vermerkt oder
5. entgegen Artikel 14 Abs. 5 einen Auszug aus dem Arbeitszeitplan oder eine Ausfertigung des Linienfahrplanes nicht mit sich führt.

§ 23

Zu widerhandlungen gegen die Verordnung (EWG) Nr. 3821/85

(1) Ordnungswidrig im Sinne des § 8 Abs. 1 Nr. 1 Buchstabe b des Fahrpersonalgesetzes handelt, wer als Unternehmer gegen die Verordnung (EWG) Nr. 3821/85 des Rates vom 20. Dezember 1985 über das Kontrollgerät im Straßenverkehr (ABl. EG Nr. L 370 S. 8), die zuletzt durch die Verordnung (EG) Nr. 432/2004 der Kommission vom 5. März 2004 (ABl. EU Nr. 71 S. 3) geändert worden ist, verstößt, indem er vorsätzlich oder fahrlässig

1. entgegen Artikel 3 Abs. 1 erster Halbsatz ein Kontrollgerät nicht einbaut oder nicht benutzt,
2. entgegen Artikel 13 für das ordnungsgemäße Funktionieren des Kontrollgerätes oder die ordnungsgemäße Benutzung des Kontrollgerätes oder der Fahrerkarte nicht sorgt,
3. entgegen Artikel 14 Abs. 1 Unterabs. 1 Satz 1 eine ausreichende Anzahl Schaublätter nicht aushändigt,
4. entgegen Artikel 14 Abs. 1 Unterabs. 1 Satz 2 ein Schaublatt aushändigt, das sich für das eingebaute Kontrollgerät nicht eignet,
5. entgegen Artikel 14 Abs. 1 Unterabs. 2 nicht dafür Sorge trägt, dass der dort genannte Ausdruck ordnungsgemäß erfolgen kann,
6. entgegen Artikel 14 Abs. 2 Satz 1 erster Halbsatz oder Satz 2 ein Schaublatt nicht oder nicht mindestens ein Jahr aufbewahrt, nicht oder nicht rechtzeitig vorlegt oder nicht oder nicht rechtzeitig aushändigt oder
7. entgegen Artikel 16 Abs. 1 Unterabs. 1, auch in Verbindung mit Unterabs. 2, eine Reparatur nicht, nicht richtig oder nicht rechtzeitig durchführen lässt.

(2) Ordnungswidrig im Sinne des § 8 Abs. 1 Nr. 2 Buchstabe b des Fahrpersonalgesetzes handelt, wer als Fahrer gegen die Verordnung (EWG) Nr. 3821/85 verstößt, indem er vorsätzlich oder fahrlässig

1. entgegen Artikel 3 Abs. 1 erster Halbsatz ein Kontrollgerät nicht benutzt,
2. entgegen Artikel 13 für das ordnungsgemäße Funktionieren des Kontrollgerätes oder die ordnungsgemäße Benutzung des Kontrollgerätes oder der Fahrerkarte nicht sorgt,
3. entgegen Artikel 14 Abs. 1 Unterabs. 2 nicht dafür Sorge trägt, dass der dort genannte Ausdruck ordnungsgemäß erfolgen kann,
4. entgegen Artikel 14 Abs. 4 Buchstabe a Unterabs. 3 Satz 2 oder 3 eine andere Fahrerkarte, eine defekte Fahrerkarte oder eine Fahrerkarte, deren Gültigkeit abgelaufen ist, benutzt,
5. entgegen Artikel 15 Abs. 1 Unterabs. 1 Satz 1 oder Abs. 2 Unterabs. 1 Satz 2 oder 3 ein Schaublatt oder eine Fahrerkarte verwendet oder entnimmt,
6. entgegen Artikel 15 Abs. 2 Unterabs. 1 Satz 1 ein Schaublatt oder eine Fahrerkarte nicht benutzt,
7. entgegen Artikel 15 Abs. 2 Unterabs. 2 oder 3 oder Abs. 5 eine Eintragung oder eine Änderung nicht, nicht richtig, nicht vollständig, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig vornimmt,
8. einer Vorschrift des Artikels 15 Abs. 3 über die Zeitmarkierung auf dem Schaublatt oder das Betätigen der Schaltvorrichtung des Kontrollgerätes zuwiderhandelt,
9. entgegen Artikel 15 Abs. 5a Unterabs. 1 Satz 1 ein Symbol nicht oder nicht richtig eingibt,
10. entgegen Artikel 15 Abs. 7 Unterabs. 1 oder 2 ein Schaublatt, die Fahrerkarte oder einen Ausdruck nicht oder nicht rechtzeitig vorlegt,

11. entgegen Artikel 16 Abs. 2 Unterabs. 1 eine dort genannte Angabe nicht, nicht richtig, nicht vollständig oder nicht für die vorgeschriebene Dauer vermerkt,
12. entgegen Artikel 16 Abs. 2 Unterabs. 2 eine Angabe nicht oder nicht rechtzeitig ausdrucken lässt oder nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht oder den Ausdruck nicht oder nicht rechtzeitig mit der Unterschrift versieht oder
13. entgegen Artikel 16 Abs. 3 Unterabs. 3 die Fahrt ohne Fahrerkarte fortsetzt.

(3) Ordnungswidrig im Sinne des § 8 Abs. 1 Nr. 4 Buchstabe b des Fahrpersonalgesetzes handelt, wer als Werkstattinhaber oder als Installateur vorsätzlich oder fahrlässig entgegen Artikel 12 Abs. 1 Unterabs. 1 der Verordnung (EWG) Nr. 3821/85 ein Kontrollgerät einbaut oder repariert.

§ 24 Zuwiderhandlungen gegen die Verordnung (EG) Nr. 2135/98

Ordnungswidrig im Sinne des § 8 Abs. 1 Nr. 2 Buchstabe b des Fahrpersonalgesetzes handelt, wer als Fahrer vorsätzlich oder fahrlässig entgegen Artikel 2 Abs. 4 der Verordnung (EG) Nr. 2135/98 des Rates vom 24. September 1998 zur Änderung der Verordnung (EWG) Nr. 3821/85 über das Kontrollgerät im Straßenverkehr und der Richtlinie 88/599/EWG über die Anwendung der Verordnungen (EWG) Nr. 3820/85 und (EWG) Nr. 3821/85 (ABl. EG Nr. L 274 S. 1), die durch die Verordnung (EG) Nr. 1360/ 2002 der Kommission vom 13. Juni 2002 (ABl. EG Nr. L 207 S. 1) geändert worden ist, eine Angabe nicht oder nicht rechtzeitig ausdrückt oder nicht oder nicht rechtzeitig überträgt oder das ausgedruckte Dokument nicht oder nicht rechtzeitig unterzeichnet.

§ 25 Zuwiderhandlungen gegen das AETR

(1) Ordnungswidrig im Sinne des § 8 Abs. 1 Nr. 1 Buchstabe b des Fahrpersonalgesetzes handelt, wer als Unternehmer gegen das Europäische Übereinkommen über die Arbeit des im internationalen Straßenverkehr beschäftigten Fahrpersonals (AETR) in der Fassung der Bekanntmachung vom 31. Juli 1985 (BGBl. 1985 II S. 889), zuletzt geändert durch das Gesetz vom 18. August 1997 (BGBl. 1997 II S. 1550), verstößt, indem er vorsätzlich oder fahrlässig

1. entgegen Artikel 5 einen Fahrer einsetzt, der die dort genannten Voraussetzungen nicht erfüllt,
2. entgegen Artikel 10 Abs. 1 Buchstabe e das Kontrollgerät nicht oder nicht rechtzeitig in Stand setzt,
3. entgegen Artikel 10 Abs. 2 ein dort genanntes Schaublatt nicht aushändigt,
4. entgegen Artikel 10 Abs. 3 ein Schaublatt nicht, nicht in der vorgeschriebenen Weise oder nicht mindestens zwölf Monate aufbewahrt oder den Kontrollorganen nicht oder nicht rechtzeitig vorlegt,
5. entgegen Artikel 11 Abs. 1 in Verbindung mit Artikel 6 Abs. 1 Satz 1 oder 3 oder Abs. 2, Artikel 7 Abs. 1 oder 3 Satz 1 oder Artikel 8 Abs. 1, 2, 6 oder 8 Satz 2 den Fahrbetrieb nicht so einrichtet, dass die Mitglieder des Fahrpersonals die Lenkzeiten, die Lenkzeitunterbrechungen oder die Ruhezeiten einhalten können,
6. entgegen Artikel 11 Abs. 2 Satz 2 einen festgestellten Verstoß gegen das Übereinkommen nicht oder nicht rechtzeitig abstellt oder eine dort genannte Maßnahme nicht oder nicht rechtzeitig trifft oder
7. entgegen Artikel 10 des Anhangs zum AETR für das ordnungsgemäße Funktionieren oder die richtige Verwendung des Kontrollgerätes nicht sorgt.

(2) Ordnungswidrig im Sinne des § 8 Abs. 1 Nr. 2 Buchstabe b des Fahrpersonalgesetzes handelt, wer als Fahrer gegen das Europäische Übereinkommen über die Arbeit des im internationalen Straßenverkehr beschäftigten Fahrpersonals (AETR) verstößt, indem er vorsätzlich oder fahrlässig

1. entgegen Artikel 5 ein Fahrzeug führt, ohne das dort festgelegte Mindestalter erreicht zu haben oder ohne den dort festgesetzten Anforderungen zu entsprechen,
2. entgegen Artikel 6 Abs. 1 Satz 1 oder 3 oder Abs. 2, Artikel 7 Abs. 1 oder 3 Satz 1 oder Artikel 8 Abs. 1, 2, 6 oder 8 Satz 2 Lenkzeiten, Lenkzeitunterbrechungen oder Ruhezeiten nicht einhält,
3. entgegen Artikel 9 Satz 2 Art oder Grund einer Abweichung nicht vermerkt,

FPers 2.2.1

4. entgegen Artikel 10 Abs. 1 Buchstabe b oder c Zeiten der beruflichen Tätigkeiten oder Ruhezeiten auf dem Schaublatt nicht, nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise vermerkt,
5. entgegen Artikel 10 Abs. 1 Buchstabe d ein dort genanntes Schaublatt nicht mit sich führt oder nicht vorlegt,
6. entgegen Artikel 10 Abs. 1 Buchstabe e für den ordnungsgemäßen Betrieb oder das Bedienen des Kontrollgerätes nicht sorgt oder das Kontrollgerät nicht oder nicht rechtzeitig in Stand setzt,
7. entgegen Artikel 11 Abs. 1 Satz 1 oder 3 des Anhangs zum AETR ein angeschmutztes oder beschädigtes Schaublatt verwendet oder dem Reserveblatt das beschädigte Schaublatt nicht beifügt,
8. entgegen Artikel 11 Abs. 2 Satz 1 des Anhangs zum AETR ein Schaublatt nicht benutzt,
9. entgegen Artikel 11 Abs. 2 Satz 2 oder 3 des Anhangs zum AETR ein Schaublatt entnimmt oder über den Zeitraum, für den es bestimmt ist, hinaus verwendet oder
10. entgegen Artikel 11 Abs. 2 Satz 5 des Anhangs zum AETR eine Änderung nicht oder nicht in der vorgeschriebenen Weise vornimmt.

(3) Ordnungswidrig im Sinne des § 8 Abs. 1 Nr. 4 Buchstabe b des Fahrpersonalgesetzes handelt, wer als Werkstattinhaber oder als Installateur vorsätzlich oder fahrlässig entgegen Artikel 9 Abs. 1 des Anhangs zum Europäischen Übereinkommen über die Arbeit des im internationalen Straßenverkehr beschäftigten Fahrpersonals (AETR) ein Kontrollgerät einbaut oder repariert.

Abschnitt 9 Übergangsvorschriften

§ 26

Kontrollgerätkarten, die vor Inkrafttreten dieser Verordnung von den zuständigen Behörden oder Stellen in einem vom Bundesministerium für Verkehr, Bau- und Wohnungswesen geregelten Verfahren erteilt worden sind, gelten als wirksam erteilt im Sinne der §§ 4, 5, 7 und 9 dieser Verordnung.

Hinweis der ZSV:

Diese Verordnung ist am 02. Juli 2005 in Kraft getreten.

Anlage 1
(zu § 1 Abs. 6)

1. Name, Vorname		2. Amtliches Kennzeichen												3. Tageskontrollblatt Nr.												4. Datum											
5. <input type="checkbox"/>	1	2	3	4	5	6	7	8	9	10	11	12																									
6. <input type="checkbox"/>																																					
7. <input checked="" type="checkbox"/>																																					
5. <input type="checkbox"/>	13	14	15	16	17	18	19	20	21	22	23	24																									
6. <input type="checkbox"/>																																					
7. <input checked="" type="checkbox"/>																																					
8. Ort der Fahraufnahme												9. Ort der Fahrtbeendigung												Stundenzahl													
10. Kilometerstand												bei Fahrtende												km													
Gesamtfahrstrecke:												bei Fahrtbeginn												km													
																								5. <input checked="" type="checkbox"/>													
																								6. <input type="checkbox"/>													
																								7. <input checked="" type="checkbox"/>													
Bemerkungen und Unterschrift																																					

Erläuterungen: 5. = Ruhezeiten und Lenkzeitunterbrechungen
 6. = Lenkzeiten
 7. = Sonstige Arbeitszeiten einschließlich Arbeitsbereitschaft

FPers 2.2.1

Anlage 2 (zu § 3)

Digitales Tachographensystem im Straßenverkehr Zertifizierungs-Policy für die Bundesrepublik Deutschland Version 1.0 in der Fassung vom 23. Februar 2005

1 Einleitung

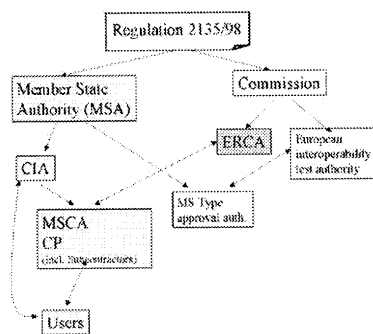
Dieses Dokument ist die Zertifizierungs-Policy der Zertifizierungsstelle der Bundesrepublik Deutschland, im Folgenden kurz als **die CA-Policy** bezeichnet, für den elektronischen Fahrtenschreiber gemäß VO(EWG) 3821/85 und Anlage 11 des Anhangs I (B) der VO(EG) 2135/98 in Verbindung mit VO(EG) 1360/2002 (CSM 008). Die vorgenannte Zertifizierungsstelle wird als D-CA bezeichnet.

Die CA-Policy befindet sich im Einklang mit der

- Digital Tachograph System - European Root Policy (Version 2.0 Special Publication 1.04.131)
- VO (EWG) 3821/85
- VO(EG) 2135/98
- VO(EG) 1360/2002
- „Common Security Guideline“.

1.1 Zuständige Organisationen

Das Tachographen-System verfügt über folgende Organisation¹⁾:



Die für die Umsetzung der VO(EWG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 in Deutschland zuständige Stelle wird im Folgenden dem internationalen Sprachgebrauch folgend mit **D-MSA** (Deutschland-Member State Authority) bezeichnet und vom Bundesministerium für Verkehr, Bau- und Wohnungswesen wahrgenommen. Offizieller Ansprechpartner ist:

Bundesministerium für Verkehr, Bau- und Wohnungswesen
Referat S 35
Robert-Schuman-Platz 1
53175 Bonn.

Die D-MSA beauftragt das Kraftfahrt-Bundesamt (KBA) mit der Wahrnehmung der Aufgaben der D-CA. Dazu gehört insbesondere die Verantwortung für die Umsetzung der CA-Policy. Die D-CA kann die Erfüllung (von Teilen) ihrer Aufgaben externen Dienstleistern übertragen. Hierdurch wird die Verantwortung der D-CA in keiner Weise eingeschränkt.

Die Wahrnehmung der Aufgaben der **D-CIA** wird von den Bundesländern jeweils individuell bestimmt.

Der **D-CP** wird von der D-MSA bestimmt.

¹⁾ Guideline and Template National CA policy, V 1.0.

1.2 Genehmigung

Die deutsche CA-Policy wurde von der D-MSA bei der EU-Kommission zur Genehmigung vorgelegt und durch die Europäische Behörde am 9. Februar 2005 genehmigt²⁾.

1.3 Verfügbarkeit und Kontakt-Details

Die nationale CA Policy steht in elektronischer Form auf der Web-Seite <http://www.kba.de> zur Verfügung. Fragen und Kontakt-Details zu dieser nationalen CA Policy sind zu richten an:

Bundesministerium für Verkehr, Bau- und Wohnungswesen
Referat S 35
Robert-Schuman-Platz 1
53175 Bonn.

2 Geltungsbereich

[r2.1]

Die Gültigkeit der CA-Policy erstreckt sich ausschließlich auf die Wahrnehmung der Aufgaben im Rahmen der VO(EWG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002.

[r2.2]

D-MSA und D-CA stellen im Rahmen ihrer jeweiligen Zuständigkeiten und der jeweils geltenden Rechtsvorschriften sicher, dass die von der D-CA erstellten Zertifikate und Schlüssel nur für die in der VO(EWG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 definierten Zwecke im Rahmen ihrer individuellen Zuständigkeiten und den relevanten gültigen Regelungen eingesetzt werden.

[r2.3]

Der Geltungsbereich der vorliegenden deutschen Policy ist in folgender Übersicht fett markiert³⁾:

3 Allgemeine Regelungen

3.1 Aufgaben und Verpflichtungen

Dieser Abschnitt beschreibt Aufgaben und Verpflichtungen der an der Umsetzung der VO(EWG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 beteiligten Stellen, soweit diese den Gültigkeitsbereich der CA-Policy betreffen.

[r3.1]

Die **D-MSA**

- a) nimmt ihre Aufgaben in Abstimmung mit den Ländern wahr,
- b) ist zuständig für die Erstellung und Aktualisierung der CA-Policy und veranlasst deren Genehmigung durch die Kommission,
- c) ernennt die D-CA und gibt diese Ernennung der Generaldirektion für Verkehr und Energie der Europäischen Union (DG TREN) bekannt,
- d) ernennt den D-CP oder lagert diese Aufgabe an einen externen Dienstleister aus,
- e) kann Überprüfungen der D-CA, der D-CP, der D-CIA, der Hersteller und weiterer externer Dienstleister durchführen oder veranlassen, wenn dies erforderlich ist,
- f) stellt sicher oder veranlasst, dass die D-CA alle für ihre Tätigkeit benötigten Informationen in korrekter Weise erhält,

2) Genehmigt wurde die Fassung in englischer Sprache, die bei Zweifelsfragen Vorrang vor der deutschen Fassung hat.

3) Vgl. Digital Tachograph System European Root Policy, V 2.0.

FPers 2.2.1

- g) genehmigt das Practice Statement (PS) der D-CA und ggf. das PS weiterer externer Dienstleister,
- h) stellt sicher oder veranlasst, dass die CA-Policy den beteiligten Stellen zur Verfügung gestellt wird,
- i) informiert unverzüglich die ERCA oder eine ihrer autorisierten Stellen über alle sicherheitsrelevanten Vorfälle bei der Produktion, Personalisierung und beim Einsatz ihrer Geräte sowie der in diese eingebrachten Schlüssel und Zertifikate.

[r3.2]

Die D-CA

- a) führt in ihrem Betrieb die Anforderungen der VO(EWG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002, aller hierfür relevanten Rechtsvorschriften, der Root-Policy und dieser CA-Policy aus,
- b) erstellt ein PS, in dem mindestens die Art der Umsetzung der CA-Policy, der Root-Policy und der gesetzlichen Regelungen erläutert wird,
- c) hält die zur ordnungsgemäßen Erfüllung ihrer Aufgabe notwendigen personellen und materiellen Ressourcen bereit,
- d) trägt die Verantwortung für die ordnungsgemäße Durchführung ihrer Aufgaben auch dann, wenn sie diese oder Teile davon an externe Dienstleister auslagert. In diesem Fall hat sie sicherzustellen, dass diese in ihrem Betrieb die relevanten Anforderungen der CA-Policy und des PS einhalten,
- e) informiert unverzüglich die D-MSA oder eine ihrer autorisierten Stellen über alle sicherheitsrelevanten Vorfälle bei der Produktion, Personalisierung und beim Einsatz ihrer Geräte sowie der in diese eingebrachten Schlüssel und Zertifikate.

[r3.3]

Die D-CIA

- a) stellt sicher, dass die Antragsdaten korrekt und entsprechend den Anforderungen der D-CA an die D-CA und den D-CP geliefert werden,
- b) informiert in geeigneter Weise alle Nutzer über die Anforderung dieser Policy,
- c) prüft, ob alle Voraussetzungen für die Ausgabe einer Karte gegeben sind,
- d) stellt sicher, dass die PIN der Werkstattkarte nur an die Person ausgeliefert wird, für die die Werkstattkarte ausgestellt wurde,
- e) informiert unverzüglich die D-MSA und die D-CA oder eine ihrer autorisierten Stellen über alle sicherheitsrelevanten Vorfälle.

[r3.4]

Der D-CP

- a) erfüllt in seinem Betrieb die Anforderungen der VO(EWG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002, aller hierfür relevanten sonstigen Rechtsvorschriften, der Root-Policy und dieser CA-Policy sowie des PS der D-CA,
- b) schließt - sofern es sich bei diesem um einen externen Dienstleister handelt - einen Vertrag mit der D-MSA ab, in dem er die Erfüllung seiner Verpflichtungen nach Buchstabe a verbindlich zusagt,
- c) weist der D-MSA gegenüber die konkrete Umsetzung seiner Verpflichtungen im laufenden Betrieb in geeigneter Weise nach,
- d) gestattet der D-MSA oder einer von ihr beauftragten Stelle, die praktische Umsetzung seiner Verpflichtungen zu überprüfen,
- e) informiert unverzüglich die D-CA oder eine ihrer autorisierten Stellen über alle sicherheitsrelevanten Vorfälle bei der Produktion, Personalisierung und beim Einsatz ihrer Geräte sowie der in diese eingebrachten Schlüssel und Zertifikate.

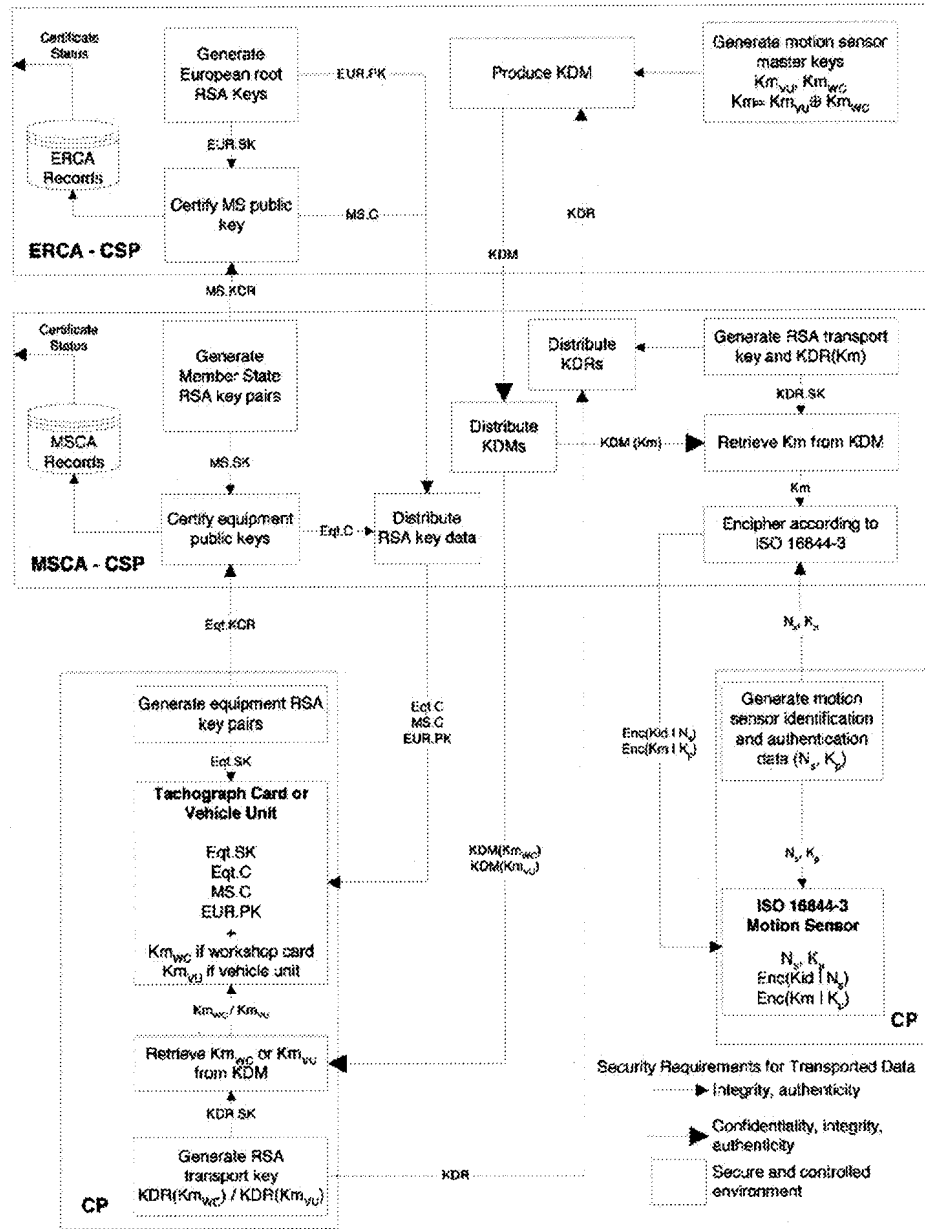


Figure 1 Description of Annex (B) key management

FPers 2.2.1

[[r3.5]

Der **Karteninhaber/Antragsteller** ist verpflichtet:

- a) wahrheitsgemäße Angaben über die Antragsdaten zu machen,
- b) bei Antragstellung wahrheitsgemäße Angaben über vorhandene Karten und Kartenarten zu machen,
- c) auf geeignete Weise sicherzustellen, dass seine Karte nur für den vorgesehenen Zweck benutzt wird und Missbrauch, insbesondere durch Dritte, verhindert wird,
- d) sicherzustellen, dass er nur in Besitz einer einzigen, gültigen Fahrerkarte ist,
- e) beschädigte und abgelaufene Karten nicht zu verwenden,
- f) Verlust, Diebstahl, Beschädigung oder Missbrauch der Karte bzw. des jeweiligen privaten Schlüssels oder den Verdacht darauf der jeweils zuständigen Stelle zu melden.

[r3.6]

Hersteller von Fahrzeugeinheiten und Hersteller von Weg-/Geschwindigkeitsgebern stellen insbesondere sicher, dass sie

- a) die für sie relevanten Anforderungen der VO(EWG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002, aller hierfür relevanten sonstigen Gesetze und Rechtsverordnungen, insbesondere dieser CA-Policy einhalten, nach bestem Wissen und dem jeweils aktuellen Stand der Technik
 - aa) dass die in die von ihnen hergestellten Geräte einzubringenden oder eingebrachten Schlüssel und Zertifikate nur für deren ordnungsgemäße Zwecke im Rahmen der VO(EWG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 genutzt werden können,
 - ab) Vorkehrungen treffen, die Geheimhaltung der privaten Schlüssel bzw. geheimen Schlüssel während des gesamten Produktionsprozesses und während der gesamten Nutzungsdauer der Geräte zu gewährleisten;
- b) der D-MSA alle ggf. mit der Wahrnehmung von wesentlichen Aufgaben im Zusammenhang mit der Produktion und der Personalisierung ihrer Geräte beauftragten externen Dienstleister nennen und diese zur Einhaltung der entsprechenden Anforderungen verpflichten. Sofern der Hersteller Aufgaben an Dritte weitergibt, bleiben seine Rechte und Pflichten davon unberührt;
- c) der D-MSA oder einer von ihr autorisierten Stelle unverzüglich alle ihnen bekannt gewordenen sicherheitsrelevanten Vorfälle im Zusammenhang mit der Produktion, Personalisierung und Nutzung ihrer Geräte sowie der in diese eingebrachten Schlüssel und Zertifikate mitteilen;
- d) der D-MSA oder einer von ihr beauftragten Stelle gestattet, die praktische Umsetzung seiner Verpflichtungen zu überprüfen;
- e) im Rahmen ihrer Möglichkeiten ausschließen, dass die ihnen zur Verfügung gestellten Schlüssel und Zertifikate in nicht bauartgenehmigte Geräte eingebaut werden;
- f) sich einem Prozess zur Aufrechterhaltung der Vertrauenswürdigkeit der ITSicherheitszertifikate nach dem BSI Zertifizierungsschema zu unterziehen. Dies beinhaltet die Überwachung der zertifizierten Produkte auf einer regelmäßigen Basis (1 Jahr) betreffend die Resistenz gegen relevante Bedrohungen in Übereinstimmung mit den Sicherheitszielen. Das BSI unterrichtet die D-MSA über die Ergebnisse.

[r3.7]

Hersteller von Kontrollgerätekarten oder Lieferanten - soweit sie IT-Sicherheitszertifikate erhalten haben - müssen sich für das Composite-Smartcard-Produkt einem Prozess zur Aufrechterhaltung der Vertrauenswürdigkeit der IT-Sicherheitszertifikate nach dem BSI Zertifizierungsschema unterziehen. Dies beinhaltet die Überwachung der zertifizierten Composite-Smartcard-Produkte auf einer regelmäßigen Basis (1 Jahr) betreffend die Resistenz gegen relevante Bedrohungen in Übereinstimmung mit den Sicherheitszielen. Das BSI unterrichtet die D-MSA über die Ergebnisse.

3.2 Besondere Rechtsvorschriften

Die D-CA und die ggf. von ihr beauftragten externen Dienstleister erfüllen ihre Aufgaben im Einklang mit geltendem Recht, insbesondere mit der VO(EWG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 und den zum Zwecke ihrer Umsetzung erlassenen nationalen Rechtsvorschriften.

Die in diesem Abschnitt genannten Rechtsvorschriften erheben *keinen* Anspruch auf Vollständigkeit.

Version 04/2005

[r3.8]

Datenschutz

Die D-CA stellt sicher, dass im Rahmen ihres Einflussbereichs die Vorschriften des Bundesdatenschutzgesetzes und entsprechender weiterer datenschutzrechtlicher Vorschriften für den Umgang mit personenbezogenen Daten eingehalten werden.

[r3.9]

Elektronische Signaturen

Die bei der D-CA produzierten Zertifikate dienen zur Verifizierung von Elektronischen Signaturen im Sinne des Gesetzes über Rahmenbedingungen für Elektronische Signaturen (Signaturgesetz). Die Zertifikate sind *nicht* qualifizierte Zertifikate im Sinne des Signaturgesetzes. Die D-CA stellt sicher, dass sie und die von ihr beauftragten externen Dienstleister die hieraus resultierenden Anforderungen (§14) des Signaturgesetzes einhalten.

4 Practice Statement der D-CA

[r4.1]

Die D-CA erstellt und pflegt ein PS, in dem in Form von konkret umzusetzenden Maßnahmen dargestellt wird, wie die Einhaltung dieser CA-Policy, der Root-Policy und der für die Tätigkeit der D-CA relevanten gesetzlichen Regelungen im Betrieb der D-CA gewährleistet ist. Dieses PS enthält eine tabellarische Übersicht, aus der ersichtlich wird, wo die Anforderungen dieser Policy im PS umgesetzt werden.

[r4.2]

Das PS muss alle externen Dienstleister der D-CA und ihre konkreten Aufgaben benennen sowie darlegen, welche der an die D-CA zu stellenden Anforderungen von diesen Dienstleistern einzuhalten sind.

[r4.3]

Das PS muss darlegen, wie die D-CA ihren Informationspflichten nachkommt.

[r4.4]

Im PS muss ein Revisionsprozess beschrieben sein, der sicherstellt, dass das PS stets dem aktuellen Stand der Gesetzgebung, der Technik und den aktuellen Gegebenheiten bei der D-CA und ihren externen Dienstleistern entspricht.

[r4.5]

Die D-CA legt der D-MSA ihr PS zur Genehmigung vor. Wesentliche Änderungen des PS bedürfen ebenfalls der Genehmigung der D-MSA. Die D-CA stellt sicher, dass die D-MSA stets über die aktuelle Version des PS verfügt.

[r4.6]

Die öffentlichen Teile des PS können außerhalb des PS in einem Realisierungskonzept (RK) beschrieben werden.

[r4.7]

Das PS enthält eine genaue Auflistung von Ereignissen, die als Verdacht auf Schlüsselkompromittierung angesehen werden. Diese Auflistung ist vertraulich zu behandeln.

Karten- und Gerätemanagement

[r5.1]

Die D-CA stellt nach den Vorgaben der D-MSA und gemeinsam mit dieser innerhalb ihres Einflussbereichs sicher, dass die von ihr produzierten Zertifikate und die von ihr ausgelieferten geheimen Schlüssel entsprechend ihrem Verwendungszweck nur in Kontrollgerätekarten und Kontrollgeräte eingebracht und eingesetzt werden, die den Anforderungen der VO(EWG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 genügen.

[r5.2]

Die D-CA verweigert die Auslieferung von Schlüsseln und Zertifikaten, wenn die Gefahr eines Missbrauchs von Schlüsseln und Zertifikaten vorliegt.

FPers 2.2.1

[r5.3]

Die D-CIA gewährleistet die Einhaltung des von der D-MSA entsprechend den Vorgaben der VO(EWG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 definierten Antrags- und Auslieferungsverfahrens für Kontrollgerätkarten.

[r5.4]

Die D-CIA stellt innerhalb ihres Einflussbereichs sicher, dass die Ausstellung von Ersatzkarten und die Kartenerneuerung nur unter den in der VO(EWG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 genannten Voraussetzungen erfolgt und dass die dafür vorgeschriebenen Fristen eingehalten werden können.

[r5.5]

Der D-CP stellt sicher, dass die Kontrollgerätkarten logisch entsprechend der Vorgaben der VO(EWG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 personalisiert werden. Dabei ist insbesondere die Integrität der aufgetragenen Daten zu wahren.

[r5.6]

Die D-CA, D-CP und Hersteller stellen innerhalb ihres jeweiligen Einflussbereichs sicher, dass private und geheime Schlüssel in einer gesicherten Produktionsumgebung aufbewahrt und eingesetzt werden.

[r5.7]

Die D-CIA stellt dem zentralen Register beim KBA die relevanten Daten zur Verfügung, damit nachvollzogen werden kann, welche Karte welchem Inhaber/Nutzer ausgestellt wurde.

[r5.8]

Die D-CIA stellt sicher, dass personalisierte Karten innerhalb der durch die VO(EWG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 vorgegebenen Fristen sicher und nachvollziehbar an ihre Inhaber/Nutzer ausgeliefert werden. Voraussetzung für die Ausstellung einer personalisierten Karte an einen Inhaber/Nutzer ist, dass dieser entweder bei Antragstellung und/oder bei Kartenübergabe persönlich identifiziert wurde. Sofern Karten nicht auf eine natürliche Person ausgestellt werden, muss der Antragsteller und der Empfänger der Karten eine ausreichende Legitimation nachweisen können.

[r5.9]

Der D-CP stellt sicher, dass Werkstattkarten mit einer PIN gemäß den Vorgaben der VO(EWG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 ausgestattet werden.

[r5.10]

Die Generierung der PIN erfolgt in einem gegen unautorisierte Zugriffe abgesicherten System. Dieses System verhindert, dass nachträglich eine Zuordnung von PIN und Werkstattkarte erfolgen kann. Die PIN wird nach ihrer Generierung auf einem angeschlossenen Drucker ausgedruckt, in einem Briefumschlag (PIN-Brief) verschlossen und nur an die Person ausgeliefert, für die die Werkstattkarte ausgestellt wurde.

Das zur PIN-Generierung und PIN-Brieferstellung benutzte System muss zumindest die Anforderungen von ITSEC E3 (mittel), Common Criteria EAL 4, oder einem äquivalenten IT Sicherheitskriterienwerk erfüllen oder nachweislich durch andere Maßnahmen eine gleichwertige Sicherheit gewährleisten.

Die Versendung der PIN-Briefe muss getrennt von den personalisierten Karten erfolgen. Sie kann auf normalem Postweg erfolgen.

[r5.12]

Die Rekonstruktion einer PIN ist auszuschließen.

6 Schlüsselmanagement in der D-CA

Dieser Abschnitt enthält Anforderungen für den Umgang der D-CA mit folgendem Schlüsselmaterial (in Klammern die in der VO(EWG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 ggf. hierfür verwendeten Kürzel):

- der öffentliche Schlüssel der Root-CA (EUR.PK),
- das Schlüsselpaar der D-CA (MS.SK, MS.PK),
- symmetrische Schlüssel für Weg-/Geschwindigkeitsgeber (K_m , $K_{m_{wc}}$, $K_{m_{vu}}$),
- ggf. Transportschlüssel zur Kommunikation mit der Root-CA und

- ggf. eigene Transportschlüssel der D-CA.

Die D-CA stellt die Vertraulichkeit und Integrität aller bei ihr erzeugten, verwendeten und/oder gespeicherten nicht öffentlicher Schlüssel sicher und verhindert wirksam jeglichen Missbrauch dieser Schlüssel. Hierzu hat sie besonders geeignete technische Systeme einzusetzen, die eine der folgenden Anforderungen erfüllen:

- FIPS 140-2 (oder 140-1); Level 3 oder höher [FIPS],
- CEN Workshop Agreement 14176-2 [CEN],
- Zertifizierung nach EAL 4 oder höher [CC] in Verbindung mit ISO 15408 [CC] oder E3 oder höher [ITSEC] auf der Grundlage eines Schutzprofils oder von Sicherheitsvorgaben („security targets“), die die Anforderungen dieser CA-Policy - basierend auf einer umfassenden Risikoanalyse - auch infrastrukturelle und nicht technische Sicherheitsmaßnahmen erfasst,
- äquivalente Sicherheitskriterien, die nachweislich eine gleichwertige Sicherheit gewährleisten.

Ebenso ist aufzuzeigen, dass diese Systeme bei der D-CA in einer ausreichend sicheren Betriebsumgebung eingesetzt werden.

6.1 Öffentlicher Schlüssel der Root-CA (EUR.PK)

[r6.1]

Die D-CA stellt sicher, dass in ihrem laufenden Betrieb Integrität und Verfügbarkeit des Schlüssels EUR.PK sichergestellt sind.

[r6.2]

Die D-CP und Hersteller stellen sicher, dass EUR.PK in alle Kontrollgerätkarten und Fahrzeugeinheiten in ihrem Einflussbereich eingebracht werden.

6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK)

[r6.3]

Die D-CA muss verschiedene Mitgliedstaatschlüsselpaare besitzen für die Produktion von öffentlichen Schlüssel-Zertifikaten für Weg-/Geschwindigkeitsgeber (unbegrenzte Gültigkeit) und öffentlichen Schlüssel-Zertifikaten für Fahrzeugeinheiten (begrenzte Gültigkeit).

[r6.4]

Die D-CA stellt sicher, dass MS.SK ausschließlich zur Signierung von Zertifikaten für Kontrollgerätkarten, Fahrzeugeinheiten und für die Produktion der ERCA Schlüsselzertifizierungsanforderung (KCR) verwendet wird. Dies beinhaltet insbesondere die Geheimhaltung des privaten Schlüssels MS.SK.

[r6.5]

Die Erzeugung des D-CA-Schlüsselpaars darf nur bei aktiver Mitwirkung von mindestens drei unterschiedlichen Personen innerhalb der D-CA erfolgen. Eine dieser Personen muss die Rolle des CA-Administrators einnehmen, die beiden anderen müssen jeweils eine andere der in dieser CA-Policy beschriebenen Rollen wahrnehmen.

[r6.6]

Die D-CA sollte - im Rahmen der Vorgaben der Root-Policy - eine angemessene Anzahl von Ersatz-Schlüsselpaaren mit den zugehörigen Zertifikaten vorhalten, um bei Nichtverfügbarkeit des aktuellen Schlüssels einen schnellen Schlüsselwechsel auch ohne aktive Mitwirkung der Root-CA durchführen zu können. Sollten mehrere aktuelle Schlüsselpaare vorliegen, stellt die D-CA sicher, dass stets der richtige Schlüssel verwendet wird.

[r6.7]

Jeder private Schlüssel MS.SK soll höchstens zwei Jahre eingesetzt werden. Nach Ende seiner Verwendungsdauer ist er von der D-CA so zu vernichten, dass ein künftiger Gebrauch oder Missbrauch ausgeschlossen ist.

[r6.8]

Die Gültigkeitsdauer der öffentlichen Mitgliedstaatschlüssel MS. PK ist unbegrenzt.

FPers 2.2.1

[r6.9]

Die D-CA hat den privaten Schlüssel und alle Ersatzschlüssel durch technisch-organisatorische Maßnahmen wirksam vor Missbrauch, Veränderung und unbefugter Kenntnisnahme zu schützen.

[r6.10]

Die D-CA verhindert durch technisch-organisatorische Maßnahmen wirkungsvoll, dass ein Zugriff auf MS.SK durch eine einzelne Person allein erfolgen kann („4-Augen-Prinzip“).

[r6.11]

Es findet keine Schlüssel hinterlegung von MS.SK statt, d.h. einschließlich Geräteschlüssel.

[r6.12]

Das PS der D-CA soll eine explizite Vorgehensweise für den Fall enthalten, dass eine Kompromittierung von MS.SK stattgefunden hat oder der begründete Verdacht dazu besteht. Diese Vorgehensweise soll auch Anweisungen an externe Dienstleister und Informationen an Kartenbesitzer und Gerätehersteller enthalten.

Im Falle, dass die Schlüssel EUR.SK, MS.SK, Km, Km_{wc}, Km_{vu} kompromittiert wurden oder der begründete Verdacht dazu besteht, sind die D-MSA und die Root-CA unverzüglich zu informieren.

In anderen Fällen von Schlüsselkompromittierung oder des begründeten Verdachts der Schlüsselkompromittierung sind geeignete Maßnahmen zu ergreifen und die betroffenen Institutionen zu informieren.

[r6.13]

Die D-CA stellt in Kooperation mit der Root-CA sicher, dass sie zu jedem Zeitpunkt über ein gültiges Schlüsselpaar (MS.SK, MS.PK) mit zugehörigem Zertifikat verfügt.

[r6.14]

Die D-CA reicht die öffentlichen Mitgliedstaatschlüssel zur Zertifizierung bei der ERCA ein unter Verwendung des Protokolls der Schlüsselzertifizierungsanforderung (KCR), wie in Anhang A der Digital Tachograph System European Root Policy beschrieben.

[r6.15]

Die D-CA erkennt den öffentlichen ERCA-Schlüssel in dem in Anhang B der Digital Tachograph System European Root Policy beschriebenen Auslieferungsformat an.

[r6.16]

Die D-CA verwendet für den Schlüssel- und Zertifikatetransport die physikalischen Medien, die im Anhang C der Digital Tachograph System European Root Policy beschrieben sind.

6.3 Symmetrische Schlüssel für Werkstattkarten und Weg-/Geschwindigkeitsgeber (Km, Km_{wc}, Km_{vu})

[r6.17]

Die D-CA fordert bei Bedarf von der Root-CA die Weg-/Geschwindigkeitsgeber-Schlüssel Km, Km_{wc}, Km_{vu} an. Für Anforderung und Auslieferung dieser Schlüssel zwischen Root-CA und D-CA sind die Bestimmungen der Root-CA einzuhalten.

[r6.18]

Die D-CA stellt durch geeignete Maßnahmen sicher, dass die Schlüssel Km_{wc} und Km_{vu} nur an die hierfür vorgesehenen Empfänger weitergegeben werden und sichert diese Weitergabe durch geeignete Maßnahmen. Die D-MSA überwacht die Sicherheitsmaßnahmen der D-CA.

Die D-CA stellt sicher, dass der Schlüssel Km nicht weitergegeben wird.

[r6.19]

Im Falle, dass eine Kompromittierung eines der Schlüssel Km_{wc} oder Km_{vu} oder insbesondere von Km stattgefunden hat oder dass der begründete Verdacht hierauf vorliegt, informiert die D-CA unverzüglich die D-MSA und die Root-CA von diesem Sachverhalt.

[r6.20]

Die D-CA fordert die Weg-/Geschwindigkeitsgeber-Schlüssel unter Verwendung des Protokolls der Schlüssel auslieferungsanforderung (KDR), beschrieben in Anhang D der ERCA-Policy, bei der ERCA an.

6.4 Transportschlüssel der Root-CA

[r6.211]

Für den Fall, dass die Root-CA der D-CA zur Absicherung der gegenseitigen Kommunikation kryptographische Schlüssel zur Verfügung stellt, so ist deren Vertraulichkeit und Integrität von der D-CA wirksam zu schützen sowie jeglicher Missbrauch wirksam zu verhindern.

6.5 Eigene Transportschlüssel der D-CA

[r6.22]

Für den Fall, dass die D-CA ihren Kommunikationspartnern (etwa Personalierer, Gerätehersteller, ...) zur Absicherung der gegenseitigen Kommunikation kryptographische Schlüssel zur Verfügung stellt, so ist deren Vertraulichkeit und Integrität von der D-CA wirksam zu schützen sowie jeglicher Missbrauch wirksam zu verhindern.

Die D-CA verpflichtet ihre Kommunikationspartner dazu, in deren Einflussbereich gleichwertige Sicherheitsvorkehrungen zum Schutz der Schlüssel zu treffen.

7 Schlüsselmanagement asymmetrischer Karten- und Geräteschlüssel

Dieser Abschnitt enthält Anforderungen für die Erzeugung und den Umgang mit asymmetrischen kryptographischen Schlüsseln für Kontrollkarten und Kontrollgeräte und die zugehörigen Zertifikate. Anforderungen für die symmetrischen Schlüssel K_m , $K_{m_{wc}}$, $K_{m_{vu}}$ finden sich in Abschnitt 6.3.

7.1 Allgemeine Anforderungen, Protokollierung

[r7.1]

Die D-MSA, D-CA, D-CP und Hersteller stellen innerhalb ihres Einflussbereichs sicher, dass Initialisierung, Beschlüsselung und Personalisierung der Karten und Kontrollgeräte in besonders abgesicherten Produktionsumgebungen erfolgen. Der Zutritt zu diesen Bereichen muss wirksam beschränkt und kontrollierbar sein. Die Administration der entsprechenden Systeme muss die Anwesenheit von mindestens zwei gemäß Rollenkonzept verantwortlichen Personen erfordern.

Jeder Zutritt zu den Systemen, jeder Zugriff auf die Systeme sowie alle von den Systemen vorgenommenen Aktionen müssen revisionssicher so protokolliert werden, dass die Verfügbarkeit und Integrität der Protokollierung auch im Falle einer Schlüsselkompromittierung sichergestellt ist.

[r7.2]

Die D-MSA, D-CA, D-CP und Hersteller stellen innerhalb ihres Einflussbereichs sicher, dass bei der Initialisierung, Beschlüsselung und Personalisierung der Karten und Kontrollgeräte sicherheitskritische Informationen wie private Schlüssel u. Ä. entsprechend der Anforderungen der VO(EWG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 und der CA-Policy geschützt werden.

[r7.3]

Die D-MSA verpflichtet etwaige externe Dienstleister dazu, die übernommenen Aufgaben vollständig getrennt von ihren sonstigen Tätigkeiten wahrzunehmen. Dies gilt insbesondere dann, wenn der Dienstleister auch für die CAs anderer Mitgliedstaaten Aufgaben übernimmt.

Die D-MSA verpflichtet etwaige externe Dienstleister dazu, ihre Tätigkeit gemäß [r7.1] revisionssicher zu protokollieren und der D-MSA auf Anforderung Einblick in die Protokollierung zu gestatten.

[r7.4]

Die bei der Personalisierung von Karten und Kontrollgeräten aufgenommenen Protokollierungen müssen eine Zuordnung der jeweiligen Aktion zur zugehörigen Karten-/Gerätenummer und zum zugehörigen Zertifikat erlauben.

FPers 2.2.1

7.2 Schlüsselerzeugung

[r7.5]

Die D-MSA, D-CA, D-CP und Hersteller stellen innerhalb ihres Einflussbereichs sicher, dass die Erzeugung der Schlüssel in einer besonders abgesicherten Produktionsumgebung erfolgt, die insbesondere die Geheimhaltung des jeweiligen privaten Schlüssels gewährleistet. Für die dabei einzusetzenden Geräte gelten die gleichen Anforderungen wie für die zur Erzeugung des Schlüsselpaars der D-CA eingesetzten Geräte.

[r7.6]

Die D-MSA, D-CA, D-CP und Hersteller stellen innerhalb ihres Einflussbereichs sicher, dass private Schlüssel unmittelbar nach ihrer Einbringung in die jeweiligen Karten oder Geräte dauerhaft aus den Speichern der Schlüsselerzeugungs- und Personalisierungssysteme gelöscht werden, sofern die Schlüsselgenerierung nicht direkt im Chip erfolgt.

[r7.7]

Die D-CA stellt sicher, dass innerhalb ihres Verantwortungsbereichs das Auftreten von Schlüsselduplikaten mit hoher Wahrscheinlichkeit ausgeschlossen ist.

[r7.8]

Die Schlüsselerzeugung kann auf Vorrat erfolgen („Batch-Verfahren“), sofern durch technisch-organisatorische Maßnahmen sichergestellt ist, dass ein Missbrauch der vorgehaltenen Schlüsselpaare wirksam verhindert wird. Der Schlüsselvorrat darf die Produktionsmenge eines Monats nicht überschreiten.

7.3 Schlüsselverwendung

[r7.9]

Die D-MSA, D-CA, D-CP und Hersteller stellen innerhalb ihres Einflussbereichs sicher, dass die jeweiligen privaten Schlüssel ausschließlich zum Zwecke ihrer Bestimmung gemäß der VO(EWG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 genutzt werden können. Dies schließt insbesondere ein, dass nach Beendigung des Personalisierungsvorgangs keine Kopien dieser Schlüssel außerhalb der gesicherten Umgebungen der Kontrollkarten und Kontrollgeräte existieren.

[r7.10]

Der D-CP stellt innerhalb seines Einflussbereichs sicher, dass nur solche Karten ausgeliefert werden, bei denen optische und logische Personalisierung jeweils korrekt auf den Karteninhaber verweisen.

[r7.11]

Von den geheimen Mitgliedstaatenschlüsseln kann ein Backup gefertigt werden unter Verwendung einer Schlüsselwiederherstellungsprozedur im 4-Augen-Prinzip.

[r7.12]

Die D-MSA, D-CA, D-CP und Hersteller stellen innerhalb ihres Einflussbereichs sicher, dass private Schlüssel nach Ablauf der Nutzungsdauer einer Kontrollkarte oder eines Kontrollgeräts nicht weiter genutzt werden können.

8 Zertifikatsmanagement

Dieser Abschnitt enthält Anforderungen an die Erstellung und Verwendung der von der D-CA erzeugten Zertifikate während des Lebenszyklus der betreffenden Kontrollgerätkarten und Kontrollgeräte.

8.1 Registrierung

[r8.1]

Die D-CIA stellt innerhalb ihres Einflussbereichs sicher, dass vor der Ausstellung eines Zertifikats eine ordnungsgemäße Registrierung in den dafür zuständigen Stellen stattgefunden hat.

[r8.2]

Insbesondere stellt dabei der D-CP sicher, dass die Registrierungsdaten eine eindeutige Zuweisung der „Certificate Holder Reference“ nach Anforderung CSM 017 aus Anlage 11 zu Anhang I (B) der VO(EG) 2135/98 ermöglicht.

[r8.3]

Sofern die Schlüsselgenerierung außerhalb der D-CA stattfindet, erstellt die D-CA das beantragte Zertifikat nur dann, wenn der Antragsteller gemäß einem vorab vereinbarten Verfahren nachgewiesen hat, dass er über den zugehörigen privaten Schlüssel verfügt. Der private Schlüssel soll dabei die gesicherte Umgebung der Schlüsselgenerierung nicht verlassen.

8.2 Zertifikatserteilung

[r8.4]

Die D-CA erstellt Zertifikate nur dann, wenn ein ordnungsgemäßer Zertifikatsantrag einer dafür bevollmächtigten Stelle vorliegt und wenn bei der Antragstellung alle Anforderungen der VO(EWG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 und alle damit zusammenhängenden Rechtsvorschriften und Vereinbarungen eingehalten worden sind.

Bei einem automatisierten Verfahren ist eine Zertifikatserstellung durch manuellen Eingriff in das System auszuschließen.

[r8.5]

Die D-CA stellt innerhalb ihres Einflussbereichs sicher, dass die von ihr erstellten Zertifikate nur an den Antragsteller übermittelt werden.

[r8.6]

Die D-CA erstellt Zertifikate nur für solche Geräte und Karten, für die eine Bauartgenehmigung ausgestellt wurde.

[r8.7]

Schlüsselzertifikats-Anforderungen, die auf dem Transport von geheimen Schlüsseln beruhen, sind nicht erlaubt.

8.3 Zertifikatgültigkeit

[r8.8]

Die Gültigkeitsdauer der von der D-CA ausgestellten Zertifikate soll die maximale Verwendungsdauer der zugehörigen Karten bzw. Geräte nicht überschreiten. Zertifikate für:

- Fahrerkarten sollen nicht länger als 5 Jahre,
- Werkstattkarten nicht länger als 1 Jahr,
- Kontrollkarten nicht länger als 5 Jahre,
- Unternehmenskarten nicht länger als 5 Jahre

gerechnet vom Zeitpunkt des Beginns der Gültigkeit der jeweiligen Karte gelten. Zertifikate für Fahrzeugeinheiten haben eine unbegrenzte Gültigkeitsdauer.

8.4 Zertifikatinhalte und -formate

[r8.9]

Inhalte und Formate der von der D-CA erstellten Zertifikate entsprechen den Anforderungen der VO(EWG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002, insbesondere den in Anlage 11 zum Anhang I (B) genannten Spezifikationen.

Die D-CA signiert alle von ihr erstellten Zertifikate mit ihrem privaten Signaturschlüssel.

FPers 2.2.1

Die D-MSA stellt sicher, dass der Key Identifier (KID) und Modulus (n) von Schlüsseln, die der ERCA zur Zertifizierung und für die Anforderung von Weg-/Geschwindigkeitsgeber-Schlüssel vorgelegt werden, einmalig innerhalb des Einflussbereichs der D-CA sind.

8.5 Informationspflichten der D-CA

[r8.10]

Die D-CA übergibt alle Zertifikatsdaten an D-CP und Hersteller, so dass Zertifikate, Geräte bzw. Karten und Karteninhaber miteinander verknüpft werden.

[r8.11]

Sofern bestimmte Stellen ein berechtigtes Interesse an speziellen, nicht öffentlichen Informationen zur Tätigkeit der D-CA oder ihrer externen Auftragnehmer haben, und keine Vorschriften oder keine Sicherheitsbedenken dieser Auskunftserteilung entgegenstehen, stellt die D-CA diese Informationen in Abstimmung mit der D-MSA schnellstmöglich und korrekt zur Verfügung.

[r8.12]

Das Betriebskonzept der D-CA ist vertraulich zu behandeln. Informationen daraus dürfen in Absprache mit der D-MSA vor Ort bei der D-CA eingesehen werden, wenn ein nachgewiesenes, berechtigtes Interesse vorliegt und die Vertraulichkeit der Informationen auch beim Empfänger hinreichend geschützt ist.

[r8.13]

Die D-CA führt die Zertifikatsstatusinformationen und stellt sie zur Verfügung.

9 Informations-Sicherheit

9.1 Informations-Sicherheitsmanagement (ISMS)

[r9.1]

Die D-CA und alle ggf. von ihr beauftragten Dienstleister etablieren ein geeignetes Informations-Sicherheitsmanagement-System (ISMS), durch das die informationstechnische Sicherheit aller für die Aufgaben der D-CA relevanten Tätigkeiten dauerhaft gewährleistet ist.

Die Vorgehensweisen sollen den Anforderungen von [ISO] 17799 sowie [GSHB] genügen.

[r9.2]

Die D-CA stellt sicher, dass für alle im Zusammenhang mit der D-CA relevanten IT- Systeme und Informationen eine Schutzbedarfsfeststellung nach [GSHB] durchgeführt wird.

[r9.3]

Für die Tätigkeit der D-CA ist ein Sicherheitskonzept zu erstellen. Dieses Konzept ist mit dem Betriebskonzept abzustimmen.

[r9.4]

Erstellung und Aktualisierung des Betriebskonzepts sind Bestandteil des Informations-Sicherheitsmanagements.

9.2 Besondere Anforderungen an das Sicherheitskonzept

Der folgende Abschnitt stellt innerhalb des Sicherheitskonzepts *besonders* zu beachtende Gesichtspunkte zusammen. Er ist *nicht* als abschließende Aufzählung von dessen Inhalten gedacht.

[r9.5]

Die D-CA stellt sicher, dass nur zuverlässiges und ausreichend qualifiziertes Personal mit den erforderlichen Tätigkeiten betraut wird. Dies gilt auch für das Personal bei externen Auftragnehmern.

[r9.6]

Die für die Tätigkeit der D-CA und ggf. externer Dienstleister eingesetzten IT Systeme müssen so betrieben werden, dass mögliche Schädigungen durch Viren und andere schadhafte Codes weitestgehend verhindert sowie die möglichen Folgen von Schäden und Störungen minimiert werden.

Die Systeme müssen über wirksame Zugangskontrollen verfügen und insbesondere die in dieser Policy und den zugehörigen Sicherheits- und Betriebskonzepten beschriebenen Rollenkonzepte wirksam implementieren.

[r9.7]

Die Initialisierung von Systemen, die den privaten Signaturschlüssel der D-CA oder die geheimen symmetrischen Schlüssel $K_{m_{vu}}$, $K_{m_{wc}}$ oder K_m enthalten, darf nur in Kooperation von zwei Personen erfolgen, die vom System vorab ausreichend sicher zu authentifizieren sind.

[r9.8]

Die D-CA soll für ihre Aufgaben vertrauenswürdige Systeme und Software einsetzen, die durch geeignete Maßnahmen wirksam gegen unautorisierte Veränderungen geschützt sind.

Sofern speziell entwickelte Soft- oder Hardware eingesetzt wird, müssen die relevanten Sicherheitsvorgaben bereits im Entwicklungsprozess nachvollziehbar berücksichtigt werden.

Bei allen Veränderungen der eingesetzten Soft- und Hardware müssen dokumentierte Kontrollmechanismen umgesetzt werden.

[r9.9]

Die innerhalb der D-CA eingesetzten Netzwerke und die dort gespeicherten und verarbeiteten Daten sind durch besondere Schutzmechanismen (wie z. B. Firewalls) gegen externe Zugriffe zu schützen.

[r9.10]

Alle sicherheitsrelevanten Aktionen und Prozesse auf den für die Tätigkeit der D-CA relevanten ITSystemen sind so zu protokollieren, dass sich der zugehörige Zeitpunkt und die entsprechenden Personen mit hinreichender Sicherheit nachvollziehen lassen. Dazu gehören zumindest:

- das Einrichten von Benutzerbereichen (Accounts),
- alle Transaktions-Anforderungen (Account des Anfordernden, Typ, Status (erfolgreich/nicht erfolgreich), Gründe für das Fehlschlagen, ...),
- Software-Installationen und -Updates,
- Hardware-Modifikationen,
- Herunterfahren und Neustarts des Systems,
- Zugriff auf Audits und Archive.

[r9.11]

Die Protokolle sind gegen Veränderung und unberechtigten Zugriff zu schützen. Sie sollen regelmäßig und anlassbezogen ausgewertet und analysiert werden.

[r9.12]

Die Protokolldaten sollen für mindestens 7 Jahre so aufgehoben werden, dass eine Auswertung während dieser Zeitspanne jederzeit möglich ist.

[r9.13]

Die D-CA erstellt einen Notfallplan, in den das Verhalten bei schwerwiegenden Notfällen wie einer Schlüsselkompromittierung oder beim Verlust oder Ausfall von relevanten Daten und/oder ITSystemen festgelegt ist.

[r9.14]

Die D-CA gewährleistet einen ausreichenden infrastrukturellen und physischen Schutz ihrer Daten und IT Systeme. Dieser umfasst insbesondere einen ausreichenden Zutrittsschutz für sicherheitsrelevante Bereiche.

Bereiche, in denen private und geheime Schlüssel erzeugt, aufbewahrt und verarbeitet werden, müssen durch besondere Maßnahmen geschützt werden.

9.3 Rollentrennung

FPers 2.2.1

[r9.15]

Durch die Einrichtung von Rollenkonzepten soll verhindert werden, dass einzelne Personen Sicherheitsvorkehrungen der D-CA umgehen. Hierzu werden den einzelnen Rollen jeweils beschränkte Rechte und Pflichten zugewiesen. Die genaue Ausgestaltung hängt von den konkreten Abläufen bei der D-CA ab und bleibt dem Betriebskonzept der D-CA vorbehalten. Folgende Rollen sind aber mindestens vorzusehen:

- D-CA-Verantwortlicher (NR),
- Key-Manager (KM),
- CA-Administrator (CAA),
- System-Administrator(SysA),
- IT-Sicherheitsbeauftragter (ISSO).

Jede dieser Rollen ist mit mindestens einer Person zu besetzen; mindestens ein Vertreter ist zu benennen. Keine Person darf gleichzeitig mehr als eine dieser Rollen wahrnehmen.

Die Inhaber dieser Rollen sind von den IT-Systemen der D-CA zuverlässig zu authentifizieren.

[r9.16]

Die NR-Rolle umfasst:

- Er ist für den sicheren und störungsfreien Betrieb der D-CA als Organisation zuständig.
- Er vertritt die Organisation nach außen und ist in der D-CA-Organisation weisungsbefugt.
- Er ist nicht direkt an der Realisierung von Geschäftsprozessen beteiligt, sondern neben der Gesamtleitung der D-CA verantwortlich für die Einhaltung und Überwachung von Sicherheitsmaßnahmen.
- Er übernimmt die Verantwortung für das Change-Management.

[r9.17]

Die KM-Rolle umfasst:

- die sichere Durchführung der Key-Management-Prozesse,
- die Erzeugung, Zertifizierung, Verwaltung und Löschung der asymmetrischen Schlüssel der D-CA sowie der symmetrischen Schlüssel, die zur Verschlüsselung von Daten der Kontrollgeräte bzw. Werkstattkarten dienen. Die Rolle Key-Manager kann nur im 4-Augen-Prinzip umgesetzt werden.

[r9.18]

Die CAA-Rolle umfasst:

- Verantwortung für den reibungslosen Betrieb der technischen Systeme der DCA.

[r9.19]

Die SysA-Rolle umfasst:

- Er ist verantwortlich für den reibungslosen Betrieb der technischen Netzwerkkomponenten der D-CA. Dies betrifft beispielsweise die Firewall-Komponenten, die VPN-Komponenten und die Verkabelung. Einstellungen auf der Firewall und auf den VPN-Gateway sind nur im 4-Augen-Prinzip gestattet.

[r9.20]

Die ISSO-Rolle umfasst:

- die Überwachung der Sicherheit aller Geschäftsprozesse im Detail und die Auswertung der Sicherheitsmaßnahmen,
- die Überwachung aller anderen Rollen, die Umsetzung der Security Policy, das Change-Management bzw. die Realisierung der Geschäftsprozesse und Anweisungen innerhalb der D-CA-Organisation,
- die Verantwortung zur Durchführung der Audits, die regelmäßig innerhalb der D-CA-Organisation vorgenommen werden müssen,
- die Verantwortung für die Erstellung und Pflege des Sicherheitskonzeptes, die Teilnahme an der Mitgliedstaatschlüssel-Generierung.

[r9.21]

Sofern die D-CA Teile ihrer Aufgaben an externe Dienstleister überträgt, müssen diese ein ihren Aufgaben entsprechendes Rollenkonzept einrichten.

10 Beendigung des D-CA-Betriebs

10.1 Verlegung der D-CA Verantwortlichkeit

Die D-MSA entscheidet über eine Verlegung der D-CA-Verantwortlichkeit. Dafür muss die D-MSA eine neue D-CA benennen. Um diese Verlegung durchzuführen, müssen die folgenden Punkte erfüllt werden.

[r10.1]

Die D-MSA stellt sicher, dass die Übertragung der Aufgaben und Pflichten an die neue D-CA in geeigneter Art und Weise zu erfolgen hat.

[r10.2]

Die alte D-CA muss alle vorhandenen D-CA-Schlüssel an die neue D-CA übertragen. Die Art und Weise wird durch die D-MSA bestimmt.

[r10.3]

Kopien von Schlüsseln jeglicher Art, die in Zusammenhang mit der alten D-CA gebracht werden können oder nicht transferiert werden konnten, müssen vernichtet werden.

11 Überprüfungen des Betriebs

11.1 D-CA

[r11.1]

Die D-MSA stellt die Durchführung von regelmäßigen und anlassbezogenen unabhängigen Überprüfungen des Betriebs der D-CA sicher. Eine entsprechende Überprüfung soll mindestens einmal jährlich erfolgen. Die D-MSA kann externe Dienstleister mit dieser Aufgabe betrauen.

Bei Überprüfungen des D-CA-Betriebs muss insbesondere die Übereinstimmung des laufenden Betriebs mit den relevanten Rechtsvorschriften, mit der D-CA-Policy sowie mit dem aktuellen Betriebskonzept und dem aktuellen IT- Sicherheitskonzept verifiziert werden.

Von der D-CA ggf. beauftragte externe Dienstleister sind in die Überprüfung einzubeziehen.

[r11.2]

Die D-MSA stellt sicher, dass die Sicherheit des Betriebs des D-CA durch die Überprüfungen nicht beeinträchtigt wird. Insbesondere stellt sie sicher, dass die Ergebnisse der Überprüfungen Unbefugten nicht zugänglich gemacht werden.

Sie verpflichtet ggf. externe Dienstleister zur Verschwiegenheit.

[r11.3]

Die D-MSA fasst die Ergebnisse der Überprüfung in einem Bericht zusammen, der die Abhilfemaßnahmen definiert, einschließlich eines Implementierungsplanes, der erforderlich ist, um die Verpflichtungen der D-MSA zu erfüllen. Der Bericht ist in englischer Sprache an die ERCA zu leiten.

[r11.4]

Sofern Überprüfungen der D-CA Schwachstellen oder Abweichungen offen gelegt haben, veranlasst die D-MSA die D-CA, diese zu beseitigen. Die D-CA berichtet der D-MSA unverzüglich über Einleitung und Abschluss dieser Maßnahmen. Die D-MSA kann eine unabhängige Überprüfung des Erfolgs dieser Maßnahmen anordnen.

11.2 D-CP und Hersteller

[r11.5]

Die Einhaltung der Sicherheitsvorschriften, insbesondere der deutschen CA-Policy sind nachzuweisen durch

- ein Zertifikat von einem vom BSI oder vergleichbaren EU-Behörden akkreditierten Prüflabor,
- mindestens einmal jährliche Audits.

Die Kosten trägt der Hersteller bzw. der D-CP

Version 04/2005

FPers 2.2.1

[r11.6]

Anlassbezogene Audits im Zusammenhang mit der VO(EWG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 können jederzeit von der D-MSA und der D-CA verlangt werden. Sollten Unregelmäßigkeiten nachgewiesen werden, trägt der Hersteller bzw. D-CP die Kosten. Andernfalls trägt die veranlassende Aufsichtsstelle die Kosten.

12 Änderungen und Anpassungen der D-CA-Policy

[r12.1]

Anträge zur Änderung der D-CA-Policy sind an die D-MSA zu richten, welche in angemessener Frist geeignete Maßnahmen zu treffen hat.

[r12.2]

Die einzigen Änderungen in der D-CA-Policy, die ohne Benachrichtigung erfolgen können, sind:

- a) redaktionelle oder Schreibfehlerkorrekturen,
- b) Änderungen in der Kontaktadresse.

13 Übereinstimmung mit der ERCA-Policy

Die Anforderungen für die deutsche CA-Policy sind in der ERCA-Policy in § 5.3 beschrieben. Die nachstehende Tabelle stellt die Verbindung zwischen den in der ERCA-Policy formulierten Anforderungen und den Anforderungen der deutschen CA-Policy dar.

Nr.	Referenz ERCA-Policy	Anforderung	Referenz D-CA-Policy
1	§ 5.3.1	The MSA Policy shall identify the entities in charge of operations.	§ 1.1 Zuständige Organisationen
2	§ 5.3.2	The MSCA key pairs for equipment key certification and for motion sensor key distribution shall be generated and stored within a device which either: <ul style="list-style-type: none"> <input type="checkbox"/> is certified to meet the requirements identified in FIPS 140-2 (or FIPS 140-1) level 3 or higher [10]; <input type="checkbox"/> is certified to be compliant with the requirements identified in the CEN Workshop Agreement 14167-2 [11]; <input type="checkbox"/> is a trustworthy system which is assured to EAL4 or higher in accordance with ISO 15408 [12]; to level E3 or higher in ITSEC [13]; or equivalent security criteria. These evaluations shall be to a protection profile or security target, <input type="checkbox"/> is demonstrated to provide an equivalent level of security. 	§ 6 Schlüsselmanagement in der D-CA (Absatz 2)
3	§ 5.3.3	Member State Key Pair generation shall take place in a physically secured environment by personnel in trusted roles under, at least dual control.	§ 6 Schlüsselmanagement in der D-CA (Absatz 3) § 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.5] § 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.101] § 7.3 Schlüsselverwendung [r7.9] § 9.2 Besondere Anforderungen an das Sicherheitskonzept [r9.71]
4	§ 5.3.4	The Member State Key Pairs shall be used for a period of at most two years starting from certification by the ERCA.	§ 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.7]
5	§ 5.3.5	The generation of new Member State Key Pairs shall take into account the one month turnaround time required for certification by the ERCA.	§ 6.2 Schlüsselpaar der D-CA (MS.SK, MSPK) [r6.131]
6	§ 5.3.6	The MSA shall submit MSCA public keys for certification by the ERCA using the key certification request (KCR) protocol described in Annex A.	§ 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [x6.14]
7	§ 5.3.7	The MSA shall request motion sensor master keys from the ERCA using the key distribution request (KDR) protocol described in Annex D.	§ 6.3 Symmetrische Schlüssel für Werkstattkarten und Weg-/Geschwindigkeitsgeber (Km, Km _{wc} , Km _{vu}) [r6.20]
8	§ 5.3.8	The VISA shall recognise the ERCA public key in the distribution format described in Annex B.	§ 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.15]

FPers 2.2.1

Nr.	Referenz ERCA-Policy	Anforderung	Referenz D-CA-Policy
9	§ 5.3.9	The MSA shall use the physical media for key and certificate transport described in Annex C.	§ 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.16]
10	§ 5.3.10	The MSA shall ensure that the Key Identifier (KId) and modulus (n) of keys submitted to the ERCA for certification are unique within the domain of the MSCA.	§ 8.4 Zertifikatinhalt und -formate [r8.91]
11	§ 5.3.11	The MSA shall ensure that expired keys are not used for any purpose. The Member State private key shall be either: destroyed so that the private key cannot be recovered or retained in a manner preventing its use.	§ 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.71]
12	§ 5.3.12	The MSA shall ensure that an equipment RSA key is generated, transported, and inserted into the equipment, in such a way as to preserve its confidentiality and integrity. For this purpose, the MSA shall <ul style="list-style-type: none"> • ensure that any relevant prescription mandated by security certification of the equipment is met; • ensure that both generation and insertion (if not on-board) takes place in a physically secured environment; • unless key generation was covered by the security certification of the equipment, ensure that specified and appropriate cryptographic key generation algorithms are used. The last two of these requirements are generation shall be met by generating equipment keys within a device which either: <ol style="list-style-type: none"> a) is certified to meet the requirements identified in FIPS 140-2 (or FIPS 140-1) level 3 or higher [91]; b) is certified to be compliant with the requirements identified in the CEN Workshop Agreement 14167-2 [10]; c) is a trustworthy system which is assured to EAL4 or higher in accordance with ISO 15408 [111]; to level E3 or higher in ITSEC [12]; or equivalent security criteria. These evaluations shall be to a protection profile or security target; d) is demonstrated to provide an equivalent level of security. 	§ 7.1 Allgemeine Anforderungen, Protokollierung [r7.1] § 7.2 Schlüsselerzeugung [r7.5]
13	§ 5.3.13	The MSA shall ensure confidentiality, integrity, and availability of the private keys generated, stored and used under control of the MSA Policy.	§ 5 Karten- und Gerätemanagement [r5.6] § 6 Schlüsselmanagement in der D-CA (Absatz 2) § 7.1 Allgemeine Anforderungen, Protokollierung [r7.2]
14	§ 5.3.14	The MSA shall prevent unauthorised use of the private keys generated, stored and used under control of the MSA Policy.	§ 6 Schlüsselmanagement in der D-CA (Absatz 2) § 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.91] § 7.2 Schlüsselerzeugung [r7.8]
15	§ 5.3.15	The Member State private keys may be backed up using a key recovery procedure requiring at least dual control.	§ 7.3 Schlüsselerzeugung [r7.11]
16	§ 5.3.16	Key certification requests that rely on transportation of private keys are not allowed.	§ 8.2 Zertifikatserteilung [r8.71]
17	§ 5.3.17	Key escrow is strictly forbidden.	§ 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.11]

Nr.	Referenz ERCA-Policy	Anforderung	ReferenzD-CA-Policy
18	§ 5.3.18	The MSA shall prevent unauthorised use of its motion sensor keys.	§ 6.3 Symmetrische Schlüssel für Werkstattkarten und Weg-/Geschwindigkeitsgeber (Km, Km _{wc} , Km _{vu}) [x6.18]
19	§ 5.3.19	The MSA shall ensure that the motion sensor master key (Km) is used only to encrypt motion sensor data for the purposes of motion sensor manufacturers. The data to be encrypted is defined in the ISO/IEC 16844-3 Standard [7].	§ 6 Schlüsselmanagement in der D-CA (Absatz 2)
20	§ 5.3.20	The motion sensor master key (Km) shall never leave the secure and controlled environment of the MSA.	§ 6.3 Symmetrische Schlüssel für Werkstattkarten und Weg-/Geschwindigkeitsgeber (Km, Km _{wc} , Km _{vu}) [x6.18]
21	§ 5.3.21	The MSA shall forward the workshop card motion sensor key (Km _{wc}) to the component personaliser (in this case, the card personalisation service), by appropriately secured means, for the sole purpose of insertion into workshop cards.	§ 6.3 Symmetrische Schlüssel für Werkstattkarten und Weg-/Geschwindigkeitsgeber (Km, Km _{wc} , Km _{vu}) [r6.18]
22	§ 5.3.22	The MSA shall forward the vehicle unit motion sensor key (Km _{vu}) to the component personaliser (in this case, a vehicle unit manufacturer), by appropriately secured means, for the sole purpose of insertion into vehicle units.	§ 6.3 Symmetrische Schlüssel für Werkstattkarten und Weg-/Geschwindigkeitsgeber (Km, Km _{wc} , Km _{vu}) [r6.18]
23	§ 5.3.23	The MSA shall maintain the confidentiality, integrity, and availability of its motion sensor key copies.	§ 6 Schlüsselmanagement in der D-CA (Absatz 2)
24	§ 5.3.24	The MSA shall ensure that its motion sensor key copies are stored within a device which either: a) is certified to meet the requirements identified in FIPS 140-2 (or FIPS 140-1) level 3 or higher [9]; b) is a trustworthy system which is assured to EAL4 or higher in accordance with ISO 15408 [11]; to level E3 or higher in ITSEC [12]; or equivalent security criteria. These evaluations shall be to a protection profile or security target.	§ 6 Schlüsselmanagement in der D-CA (Absatz 2)
25	§ 5.3.25	The MSA shall possess different Member State Key Pairs for the production of vehicle unit and tachograph card equipment public key certificates.	§ 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.3] § 7.3 Schlüsselverwendung [r7.9]
26	§ 5.3.26	The MSA shall ensure availability of its equipment public key certification service.	§ 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.6]
27	§ 5.3.27	The MSA shall only use the Member State Private Keys for: a) the production of Annex I(B) equipment key certificates using the ISOAEC 9796-2 digital signature algorithm as described in Annex I(B) Appendix 11 Common Security Mechanisms [6]; b) production of the ERCA key certification request as described in Annex A; c) issuing Certificate Revocation Lists if this method is used for providing certificate status information (see 5.3.30).	§ 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.4]
28	§ 5.3.28	The MSA shall sign equipment certificates within the same device used to store the Member State Private Keys (see 5.3.2).	§ 6 Schlüsselmanagement in der D-CA (Absatz 4)

FPers 2.2.1

Nr.	Referenz ERCA-Policy	Anforderung	Referenz D-CA-Policy
29	§ 5.3.29	Within its domain, the MSA shall ensure that equipment public keys are identified by a unique key identifier which follows the prescriptions of Annex 1(B) [61.	§ 8.4 Zertifikatinhalte und -formate [r8.9]
30	§ 5.3.30	Unless key generation and certification is performed in the same physically secured Environment, the key certification request protocol shall provide proof of origin and integrity of certification requests, without revealing the private key.	§ 8 Zertifikatsmanagement [r8.3]
31	§ 5.3.31	The MSA shall maintain and make certificate status information available.	§ 8.5 Informationspflichten der D-CA [r8.13]
32	§ 5.3.32	The validity of a tachograph card certificate shall equal the validity of the tachograph card.	§ 8.3 Zertifikatgültigkeit [r8.8]
33	§ 5.3.33	The MSA shall prevent the insertion of undefined validity certificates into tachograph cards.	§ 8.3 Zertifikatgültigkeit [r8.8]
34	§ 5.3.34	The MSA may allow the insertion of undefined valid Member State certificates into vehicle units.	§ 8.3 Zertifikatgültigkeit [r8.8]
35	§ 5.3.35	The MSA shall ensure that users of cards are identified at some stage of the card issuing process.	§ 5 Karten- und Gerätemanagement [r5.8] § 7.3 Schlüsselverwendung [r7.10]
36	§ 5.3.36	The MSA shall ensure that ERCA is notified without delay of loss, theft, or potential compromise of any MSA keys.	§ 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.12]
37	§ 5.3.37	The MSA shall implement appropriate disaster recovery mechanisms which do not depend on the ERCA response time.	§ 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.6] § 9 Informations-Sicherheit [r9.13]
38	§ 5.3.38	The MSA shall establish an information security management system (ISMS) based on a risk assessment for all the operations involved.	§ 9.1 Informations-Sicherheitsmanagement (ISMS) [r9.1]
39	§ 5.3.39	The MSA shall ensure that the policies address personnel training, clearance and roles.	§ 9.2 Besondere Anforderungen an das Sicherheitskonzept [r9.5] § 9.3 Rollentrennung [r9.15]
40	§ 5.3.40	The MSA shall ensure that appropriate records of certification operations are maintained.	§ 8.4 Zertifikatinhalte und -formate [r8.9] § 9 Informations-Sicherheit [r9.10] [r9.11] [r9.12]
41	§ 5.3.41	The MSA shall include provisions for MSA termination in the MSA Policy.	§ 10.1 Verlegung der D-CA Verantwortlichkeit
42	§ 5.3.42	The MSA Policy shall include change procedures.	§ 12 Änderungen und Anpassungen der D-CA-Policy [r12.1]
43	§ 5.3.43	The MSA audit shall establish whether the Requirements of this Section are being maintained.	§ 11.1 D-CA [r11.1] 2. Paragraph
44	§ 5.3.44	The MSA shall audit the operations covered by the approved policy at intervals of not more than 12 months.	§ 11.1 D-CA [r11.1] 1. Paragraph
45	§ 5.3.45	The MSA shall report the results of the audit as mentioned in 5.3.43 and provide the audit report, in English, to the ERCA.	§ 11.1 D-CA [r11.3]
46	§ 5.3.46	The audit report shall define any corrective actions, including an implementation schedule, required to fulfil the MSA obligations.	§ 11.1 D-CA [r11.3]

Anhang A Abkürzungen, Definitionen

BMVBW	Bundesministerium für Verkehr, Bau- und Wohnungswesen
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAA	CA-Administrator
CA-Policy	Zertifizierungs-Policy für die Bundesrepublik Deutschland für die Zertifizierungsstelle der Bundesrepublik Deutschland für den elektronischen Fahrten-schreiber gemäß Anlage 11 des Anhangs I (B) VO(EG) 2135/98
Change Management	Behandlung technischer, organisatorischer und/oder fachlicher Änderungen des Verfahrens
D-CA	Zertifizierungsstelle der Bundesrepublik Deutschland für den elektronischen Fahrtenschreiber gemäß der VO(EWG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002, Kraftfahrt-Bundesamt. Nach internationalem Sprachgebrauch (CA = certification authority)
D-CIA	Ausgabestelle
D-CP	Kartenpersonalisierer: Stelle, die asymmetrische Schlüsselpaare und die gemäß VO(EWG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 zugehörigen Zertifikate auf die in der VO(EG) 2135/98 definierten Fahrer-, Werkstoff-, Kontroll- und Unternehmenskarten aufbringt.
D-MSA	Die für die Umsetzung der EU-Richtlinie in der Bundesrepublik Deutschland verantwortliche Stelle, BMVBW. Nach internationalem Sprachgebrauch (MSA = Member State Authority)
Digitale Signatur	Verfahren zur Sicherung der Unverfälschtheit (Integrität) und zum Herkunftsnachweis (Authentizität) eines elektronischen Dokuments mittels Anwendung der asymmetrischen Kryptographie.
ERCA	Europäische Rote Zertifizierungsstelle
FE	Fahrzeugeinheiten nach Definition der VO(EWG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002.
ISMS	Informations-Sicherheitsmanagement-System
ISSO	Der Sicherheitsbeauftragte Nach internationalem Sprachgebrauch (ISSO = Information System Security Officer)

FPers 2.2.1

Karten-personalisierer	Siehe D-CP
KDR	Key Distribution Request (Schlüssel-Auslieferungsantrag für den Hauptschlüssel des Weg-/Geschwindigkeitsgebers)
KM	Der Key-Manager
NR	Der D-CA-Verantwortliche Nach internationalem Sprachgebrauch (NR = D-CA-Responsible)
Öffentlicher Schlüssel	In der asymmetrischen Kryptographie der öffentliche Teil eines Schlüssel-paars. Dieser dient meistens zur Verifizierung einer digitalen Signatur oder zur Verschlüsselung einer Nachricht. (s. auch Privater Schlüssel)
Personalisierung	Auch: logische P. Einbringung von privaten/geheimen Schlüsseln und den zugehörigen Zertifikaten in Kontrollgerätkarten und Kontrollgeräte. Diese ist zu unterscheiden von der optischen P. einer Karte, bei der Namen, Fotos u. Ä. auf den Kartenkörper aufgebracht werden.
Privater Schlüssel	In der asymmetrischen Kryptographie der private (geheime) Teil. eines Schlüssel-paars. Dieser dient meistens zur Erzeugung einer digitalen Signatur oder zur Entschlüsselung einer Nachricht. (s. auch Öffentlicher Schlüssel)
PS	Das Practice Statement der D-CA, wie es in Kapitel 4 der CA-Policy definiert ist. Im internationalen Sprachgebrauch ist dafür die Bezeichnung „Certification Practice Statement (CPS)“ gebräuchlich.
Root-CA	Die europäische Zertifizierungsstelle für den elektronischen Fahrtenschreiber gemäß der VO(EWEG)) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002.
Root-Policy	„Digital Tachograph System-European Root Policy“ erstellt vom JRC in Ispra.
RSA	Spezielles Verfahren der asymmetrischen Kryptographie. Gemäß Anlage 11 des Anhangs 1 (B) der VO(EG) 2135/98 wird im elektronischen Fahrtenschreiber das RSA-Verfahren zur Erstellung digitaler Signaturen eingesetzt.
SysA	Der Systemadministrator
VPN	Virtual Private Network
Zertifikat	In der asymmetrischen Kryptographie wird durch ein Z. die Bindung eines öffentlichen Schlüssels an eine im Z. bezeichnete Identität (Person, Organisation, Maschine, ...), die sich im Besitz des zugehörigen privaten Schlüssels befindet, bestätigt. Im Kontext der CA-Policy werden hierunter insbesondere die in Anlage 11 zum Anhang I (B) der VO(EG) 2135/98 definierten Zertifikate verstanden.

Zertifizierungs-stelle

Stelle, die ein Zertifikat ausstellt. Im Kontext der VO(EWG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 existieren die Europäische Zertifizierungsstelle (Root-CA) und die Zertifizierungsstellen der Mitgliedstaaten (für Deutschland D-CA), die die für ihre Tätigkeit benötigten Zertifikate von der Root-CA erhalten.

**Anhang B
Referenzdokumente**

- [CC] Common Criteria. ISO/IEC 15408 (1999)
- [CEN] CEN Workshop Agreement 14167-2: Cryptographic Module for CSP ...
- [FIPS] FIPS PUB 140-2. NIST
- [GSHB) BSI-IT-Grundschutzhandbuch
- [SO] ISO 17799

**Anlage 3
(zu § 4)**

Beschreibung der Speicherkarten

1. Die Speicherkarten entsprechen den Mustern nach Abschnitt IV, Anhang I B, Verordnung (EWG) Nr. 3821/85. Von den danach möglichen zusätzlichen Angaben enthält die Werkstattkarte Name und Vorname des Karteninhabers.
Fahrer-, Unternehmens- und Kontrollkarte enthalten keine fakultativen Angaben.
2. Sämtliche Speicherkarten enthalten folgende zusätzliche Sicherheitsmerkmale:
 - Nicht kopierbare Elemente in Form optisch variabler Merkmale, unter anderem in Form beugungsoptisch wirksamer Strukturen (auf Grund der geforderten Gebrauchstauglichkeit vorzugsweise unterhalb der die Kartenoberfläche bildenden Kartenschicht),
 - Integration der Führerscheindaten (einschließlich des Lichtbilds und der Unterschrift) in das Kartenmaterial mittels spezieller Sicherheitstechnik, die insbesondere in den mit Sicherheitsmerkmalen belegten Kartenschichten wirksam wird (nur für Fahrerkarten),
 - Eignung für die Echtheitsprüfung auf der ersten Kontrollebene: Die Karten müssen Sicherheitsmerkmale und -eigenschaften besitzen, die ohne zusätzliche Hilfsmittel eine sichere Echtheitsprüfung des Dokuments erlauben. Zusätzlich sollen weitere Sicherheitselemente aufgebracht werden, die eine Echtheitsprüfung mit einfachen Mitteln (UV-Lampe, Lupe usw.) ermöglichen.

- Fertigungstechnische Spezifikationen für die Kontrollgerätkarten

Die Kontrollgerätkarten müssen den folgenden Normen entsprechen¹⁾:

- SO/IEC 7810 Identifikationskarten - Physikalische Eigenschaften
- SO/IEC 7816 Identifikationskarten- Chipkarten mit Kontakten (Teil 1, 2, 3, 4 und 8)
- ISO/IEC 10373 Identifikationskarten; Prüfverfahren.

Gemäß der Leistungsbeschreibung für die Erstellung und Lieferung der Kontrollgerätkarten sind hohe Anforderungen an die Haltbarkeit und Gebrauchstauglichkeit des zu verwendenden Kartenwerkstoffs und der Karten insgesamt zu stellen. Die Herstellung der Karten und die Aufbringung der Daten muss mit Sicherheitstechniken erfolgen, die nicht allgemein zugänglich sind. Daraus ergeben sich für die Kontrollgerätkarten im Einzelnen folgende technische Spezifikationen, die sich als Auswahl der wichtigsten Sicherheitselemente

FPers 2.2.1

aus einem allgemeinen EU-Mindestsicherheitsstandard für Ausweisdokumente und bestehenden Kartenkonzepten, z. B. dem der Führerscheinkarte der Bundesrepublik Deutschland, ableiten.

Nr.	Kriterien gemäß Mindestsicherheitsstandard für Ausweisdokumente ²⁾	Auswahl	Spezifikationen für Kontrollgerätarten
1	Material		vollständig aus Polycarbonat aufgebaut, zu einer homogenen Karte laminiert, Kartenkern aus weißpigmentiertem, semitransparentem Polycarbonat, auf der Vorderseite zwei, auf der Rückseite mindestens eine transparente Polycarbonatschicht, Vorderseite für Lasergravur sensibilisiert
1.1	Materialmerkmale		
	• ohne optischen Aufheller	✓	
2	Sicherheitsdruck		
2.1	Personaldatenseite/Kartenrückseite		

¹⁾ Siehe Anhang I B Abschnitt IV.3 der Verordnung (EG) Nr. 1360/2002.

²⁾ Entschließung der im Rat vereinigten Vertreter der Regierungen der Mitgliedstaaten vom 17. Oktober 2000 hinsichtlich der Sicherung von Pässen und anderer Reisedokumente, ABl. EG Nr. C 310 S.1.

Nr.	Kriterien gemäß Mindestsicherheitsstandard für Ausweisdokumente ²⁾	Auswahl	Spezifikationen für Kontrollgerätarten
	• Textdruck	✓	Text auf Vorder- und Rückseite in Blau und EU-Symbol in Blau und Gelb entsprechend Abschnitt 2.1 und der Abbildung des Gemeinschaftsmodells in Anhang I B, Abschnitt IV .1 der Verordnung (EG) Nr. 1360/2002, Anbringung auf der Vorderseite zwischen den beiden transparenten Kartenschichten und auf der Rückseite zwischen Kartenkern und transparenter Kartenschicht
	• Guillochendruck	✓	Kombination aus zwei Druckdurchgängen 1. Druckplatte: Negativguilloche mit ausgespartem Endlostext, bestehend aus dem Kartentitel in den anderen Gemeinschaftssprachen, Flächen der Negativguilloche durch Schraffur aufgeheilt, am unteren Rand Integration einer Mikroschriftzeile in das Guillochenmotiv, Iriseinfärbung mit Farbübergängen zum linken und rechten Kartenrand hin entsprechend Abschnitt 2.1, Iriszonenverhältnis ca. 25/50/25 % der Kartenbreite 2. Druckplatte: Positivguilloche, abgepasst auf das Motiv der ersten Druckplatte, mit eingearbeiteter Konturierung des in der ersten Druckplatte ausgesparten Endlostextes, in den Aussparungen Mikroschrift mit Endlostext, einheitlich eingefärbt

	• Iriseinfärbung	✓	s. o.
	• Layout Personaldatenseite ≠:übrige Seiten	-	gleiches Guillochenmotiv auf Vorder- und Rückseite, auf der Vorderseite Aussparung des Lichtbildfeldes mit sich nach innen auflösender Überlappung des Lichtbildrandes
	• Mikroschrift	✓	je eine Endlosschriftzeile unterhalb des Kartentitels in Blau und in den jeweiligen Iris-Farben mehrfarbig am unteren Rand in das Motiv der ersten Guillochendruckplatte integriert sowie Endlostext als Füllung der mit der zweiten Guillochendruckplatte auf gebrachten konturierten Endlosschrift in Rosa bzw. Grau (s. o.), Mikroschriftgröße: je-
— — — —	Kriterien gemäß Mindestsicherheitsstandard für Ausweisdokumente²⁾	Auswahl	Spezifikationen für Kontrolligeratekarten
	• UV-Aufdruck	✓	auf der Vorderseite zwischen den beiden transparenten Kartenschichten, Fluoreszenzfarbe Rot (Anregung im langwelligen UV)
	• OVI-Aufdruck	-	
2.2	Nummerierung		
	• auf Personaldatenseite	✓	in Datenfeld 5b
	in Ausstellungstechnik	✓	Lasergravur
3	Kopierschutz/weitere Sicherheitsmerkmale		
3.1	OVD		
	• beugungsoptisch wirksame Struktur	✓	transparentes Kinegram
	• im Laminat/in der Ausweiskarte integriert oder als Overlay	✓	auf der Vorderseite innenliegend zwischen Kartenkern und darauf folgender transparenter Schicht, den Lichtbildrand überlappend
3.2	weitere Sicherheitsmerkmale		
	weitere Informationsträger	✓	kontaktbehafteter IC-Chip
4	Ausstellungstechnik		
4.1	Personalisierung		
	• Bild- und Personendaten integriert	✓	Lasergravur, die Angaben in den Datenfeldern 1, 4a/4b und 5b reliefartig auf der Kartenoberfläche fühlbar
	• Elemente zum Schutz der Einträge	✓	durch geeignete Materialbeschaffenheit ist sicherzustellen, dass die durch die Lasergra-

FPers 2.2.1

4.2	Normkonformität		
	• Maschinenlesbarkeit (ICAO 9303)	-	
	ISO/IEC 7810 und 7816	✓	

2

Erläuterung der in der Tabelle verwendeten Symbole

- Anforderungen, orientiert an der EU-Entscheidung hinsichtlich der Sicherung von Pässen und anderen Reisedokumenten vom 17. Oktober 2000
- ✓ muss in der Kontrollgerätekarte enthalten sein
- ist in der Kontrollgerätekarte nicht enthalten

²) Entscheidung der im Rat vereinigten Vertreter der Regierungen der Mitgliedstaaten vom 17. Oktober 2000 hinsichtlich der Sicherung von Pässen und anderer Reisedokumente, ABI. EG Nr. C 310 S.1.